

INTRODUCCIÓN A LA TEORÍA ANALÍTICA DE LOS NÚMEROS

T. M. APOSTOL

EDITORIAL REVERTÉ

INTRODUCCIÓN A LA TEORÍA ANALÍTICA DE LOS NÚMEROS

T. M. APOSTOL



**EDITORIAL
REVERTÉ**

Barcelona · Bogotá · Buenos Aires · Caracas · México

Título de la obra original:

**Introduction to Analytic
Number Theory**

Edición original en lengua inglesa publicada por:

Springer-Verlag, New York-Heidelberg-Berlin

Copyright © by Springer-Verlag New York Inc.

Versión española por:

Dr. José Plá Carrera

Doctor en Matemáticas, Profesor de la Facultad de Ciencias Matemáticas
de la Universidad de Barcelona

Revisada por:

Dr. Enrique Linés Escardó

Catedrático de la Facultad de Ciencias Matemáticas de la Univesidad de Madrid

Reservados todos los derechos. La reproducción total o parcial de esta obra, por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, queda rigurosamente prohibida, salvo excepción prevista en la ley. Asimismo queda prohibida la distribución de ejemplares mediante alquiler o préstamo públicos, la comunicación pública y la transformación de cualquier parte de esta publicación (incluido el diseño de la cubierta) sin la previa autorización de los titulares de la propiedad intelectual y de la Editorial. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (Art. 270 y siguientes del Código Penal). El Centro Español de Derechos Reprográficos (CEDRO) vela por el respeto a los citados derechos.

Edición en papel:

ISBN: 978-84-291-5006-3

Edición e-book (PDF):

ISBN: 978-84-291-9105-9

Prólogo

Éste constituye el primero de dos volúmenes de un libro de texto¹ que deriva de un curso (Matemáticas 160) ofrecido en el California Institute of Technology durante los últimos 25 años. Proporciona una introducción a la Teoría analítica de números apropiada para estudiantes de Licenciatura con cierto conocimiento del Cálculo superior, pero que carecen de todo conocimiento de Teoría de números. En realidad, gran parte del libro no requiere Cálculo alguno y puede ser estudiado con provecho por los estudiantes de Escuelas superiores sofisticadas.

La Teoría de números es tan basta y rica que un curso no puede hacer justicia a todas sus partes. Problemas que han fascinado a generaciones de matemáticos aficionados y profesionales se discuten junto con algunas de las técnicas para resolverlos.

Una de las metas de este curso consiste en nutrir el interés intrínseco que todos los estudiantes jóvenes de matemáticas parecen tener por la Teoría de números y abrirles algunas puertas a la literatura periódica corriente. Ha resultado grato comprobar que muchos de los estudiantes que han seguido este curso durante los 25 años pasados son matemáticos profesionales, y alguno ha aportado contribuciones notables por sí mismo a la Teoría de números. Este libro va dedicado a todos ellos.

¹ El segundo volumen está a punto de aparecer en la Springer-Verlag Series Graduate Texts in Mathematics bajo el título de *Modular Functions and Dirichlet Series in Number Theory* (En el momento de efectuar la traducción ya ha hecho su aparición. N. d. t.)

Índice analítico

Introducción histórica

Capítulo 1

El teorema fundamental de la Aritmética

- 1.1 Introducción 15
- 1.2 Divisibilidad 16
- 1.3 Máximo común divisor 17
- 1.4 Números primos 19
- 1.5 El teorema fundamental de la Aritmética 20
- 1.6 La serie de los inversos de los primos 22
- 1.7 El algoritmo de Euclides 23
- 1.8 El máximo común divisor de más de dos números 24
- Ejercicios del capítulo 1 25*

Capítulo 2

Funciones aritméticas y producto de Dirichlet

- 2.1 Introducción 29
- 2.2 La función de Möbius $\mu(n)$ 29
- 2.3 La función indicatriz de Euler $\varphi(n)$ 30
- 2.4 Una relación que conecta φ y μ 32
- 2.5 Una fórmula producto para $\varphi(n)$ 32
- 2.6 El producto de Dirichlet de funciones aritméticas 35
- 2.7 Inversos de Dirichlet y fórmula de inversión de Möbius 37
- 2.8 La función de Mangoldt $\Lambda(n)$ 39
- 2.9 Funciones multiplicativas 41
- 2.10 Funciones multiplicativas y producto de Dirichlet 43
- 2.11 La inversa de una función completamente multiplicativa 44
- 2.12 La función $\lambda(n)$ de Liouville 46
- 2.13 Las funciones divisor $\sigma_a(n)$ 47

- 2.14 Convolutiones generalizadas 48
- 2.15 Series formales de potencias 50
- 2.16 La serie de Bell de una función aritmética 52
- 2.17 Series de Bell y producto de Dirichlet 54
- 2.18 Derivadas de funciones aritméticas 56
- 2.19 La identidad de Selberg 57
- Ejercicios del capítulo 2* 58

Capítulo 3

Medias de funciones aritméticas

- 3.1 Introducción 65
- 3.2 La notación O mayúscula. Igualdad asintótica de las funciones 66
- 3.3 Fórmula de sumación de Euler 67
- 3.4 Algunas fórmulas asintóticas elementales 69
- 3.5 El orden medio de $d(n)$ 72
- 3.6 El orden medio de las funciones divisor $\sigma_a(n)$
- 3.7 El orden medio de $\varphi(n)$
- 3.8 Una aplicación a la distribución de los puntos reticulares visibles desde el origen 78
- 3.9 El orden de $\mu(n)$ y de $\Lambda(n)$ 81
- 3.10 Las sumas parciales de un producto de Dirichlet 82
- 3.11 Aplicaciones a $\mu(n)$ y $\Lambda(n)$ 83
- 3.12 Otra identidad para las sumas parciales de un producto de Dirichlet 87
- Ejercicios del capítulo 3* 88

Capítulo 4

Algunos teoremas elementales sobre la distribución de los números primos

- 4.1 Introducción 93
- 4.2 Las funciones de Chebyshev $\psi(x)$ y $\vartheta(x)$ 94
- 4.3 Relaciones que ligan $\vartheta(x)$ y $\pi(x)$ 96
- 4.4 Ciertas formas equivalentes del teorema del número primo 99
- 4.5 Desigualdades relativas a $\pi(x)$ y a p_n 103
- 4.6 Teorema tauberiano de Shapiro 107
- 4.6 Aplicaciones del teorema de Shapiro 111
- 4.8 Una fórmula asintótica para las sumas parciales $\sum_{p \leq x} (1/p)$ 113
- 4.9 Las sumas parciales de la función de Möbius 114
- 4.10 Breve esbozo de una demostración elemental del teorema del número primo 124
- 4.11 Fórmula asintótica de Selberg 125
- Ejercicios del capítulo 4* 128

Capítulo 5

Congruencias

- 5.1 Definición y propiedades básicas de las congruencias 135
- 5.2 Clases de restos y sistemas completos de restos 139
- 5.3 Congruencias lineales 140
- 5.4 Sistemas residuales reducidos y el Teorema de Euler/Fermat 143
- 5.5 Congruencias polinómicas módulo p . Teorema de Lagrange 145
- 5.6 Aplicaciones del teorema de Lagrange 146
- 5.7 Congruencias lineales simultáneas. El teorema del resto chino 148
- 5.8 Aplicaciones del teorema del resto chino 149
- 5.9 Congruencias polinómicas relativas a potencias de primos 152
- 5.10 El principio de la clasificación cruzada 155
- 5.11 Una propiedad de descomposición de los sistemas residuales reducidos 157
- Ejercicios del capítulo 5* 159

Capítulo 6

Grupos abelianos finitos y sus caracteres

- 6.1 Definiciones 163
- 6.2 Ejemplos de grupos y subgrupos 164
- 6.3 Propiedades elementales de los grupos 164
- 6.4 Construcción de subgrupos 166
- 6.5 Caracteres de grupos abelianos finitos 168
- 6.6 El grupo de los caracteres 170
- 6.7 Relaciones de ortogonalidad para caracteres 171
- 6.8 Caracteres de Dirichlet 173
- 6.9 Sumas que contienen caracteres de Dirichlet 176
- 6.10 La no anulación de $L(1, \chi)$ para χ no principal real 177
- Ejercicios del capítulo 6* 180

Capítulo 7

Teorema de Dirichlet relativa a los primos que se encuentran en progresiones aritméticas

- 7.1 Introducción 183
- 7.2 Teorema de Dirichlet para primos de la forma $4n-1$ y $4n+2$
- 7.3 Plan de la demostración del teorema de Dirichlet 185
- 7.4 Demostración del lema 7.4 188
- 7.5 Demostración del lema 7.5 189
- 7.6 Demostración del lema 7.6 191
- 7.7 Demostración del lema 7.8 191

- 7.8 Demostración del lema 7.7 192
- 7.9 Distribución de primos en progresiones aritméticas 193
- Ejercicios del capítulo 7* 195

Capítulo 8

Funciones aritméticas periódicas y sumas de Gauss

- 8.1 Funciones periódicas de módulo k 197
- 8.2 Existencia de series finitas de Fourier para funciones aritméticas periódicas 198
- 8.3 Suma de Ramanujan y generalizaciones 201
- 8.4 Propiedades multiplicativas de las sumas $s_k(n)$ 204
- 8.5 Sumas de Gauss asociadas a caracteres de Dirichlet 207
- 8.6 Caracteres de Dirichlet con sumas de Gauss no nulas 208
- 8.7 Módulos inducidos y caracteres primitivos 210
- 8.8 Otras propiedades de los módulos inducidos 211
- 8.9 El conductor de un carácter 214
- 8.10 Caracteres primitivos y sumas de Gauss separables 214
- 8.11 La serie finita de Fourier de los caracteres de Dirichlet 215
- 8.12 Desigualdad de Pólya para sumas parciales de caracteres primitivos 216
- Ejercicios del capítulo 8* 219

Capítulo 9

Restos cuadráticos y ley de reciprocidad cuadrática

- 9.1 Restos cuadráticos 223
- 9.2 El símbolo de Legendre y sus propiedades 225
- 9.3 Cálculo de $(-1/p)$ y $(2/p)$ 227
- 9.4 Lema de Gauss 228
- 9.5 La ley de reciprocidad cuadrática 231
- 9.6 Aplicaciones a la ley de reciprocidad 234
- 9.7 El símbolo de Jacobi 235
- 9.8 Aplicaciones a las ecuaciones diofánticas 238
- 9.9 Sumas de Gauss y ley de reciprocidad cuadrática 240
- 9.10 Ley de reciprocidad para sumas cuadráticas de Gauss 244
- 9.11 Otra demostración de la ley de reciprocidad cuadrática 251
- Ejercicios del capítulo 9* 251

Capítulo 10

Raíces primitivas

- 10.1 El exponente de un número mod m . Raíces primitivas 255

- 10.2 Raíces primitivas y sistemas residuales reducidos 256
- 10.3 La no existencia de raíces primitivas mod 2^α para $\alpha \geq 3$ 257
- 10.4 La existencia de raíces primitivas mod p para primos impares p 258
- 10.5 Raíces primitivas y restos cuadráticos 260
- 10.6 La existencia de raíces primitivas mod p^α 260
- 10.7 La existencia de raíces primitivas mod $2p^\alpha$ 263
- 10.8 La no existencia de raíces primitivas en los restantes casos 263
- 10.9 El número de raíces primitivas mod m 265
- 10.10 Cálculo de índices 167
- 10.11 Raíces primitivas y caracteres de Dirichlet 272
- 10.12 Caracteres de Dirichlet mod p^α con valores reales 274
- 10.13 Caracteres de Dirichlet primitivos mod p^α 275
- Ejercicios del capítulo 10* 277

Capítulo 11

Series de Dirichlet y productos de Euler

- 11.1 Introducción 279
- 11.2 El semiplano de convergencia absoluta de una serie de Dirichlet 280
- 11.3 La función definida por una serie de Dirichlet 281
- 11.4 Multiplicación de series de Dirichlet 283
- 11.5 Productos de Euler 286
- 11.6 El semiplano de convergencia de una serie de Dirichlet 289
- 11.7 Propiedades analíticas de las series de Dirichlet 292
- 11.8 Series de Dirichlet con coeficientes no negativos 294
- 11.9 Series de Dirichlet expresadas como exponenciales de series de Dirichlet 296
- 11.10 Fórmulas de valor medio para series de Dirichlet 298
- 11.11 Una fórmula integral para los coeficientes de una serie de Dirichlet 300
- 11.12 Una fórmula integral para las sumas parciales de una serie de Dirichlet 302
- Ejercicios del capítulo 11* 306

Capítulo 12

Las funciones $\zeta(s)$ y $L(s, \chi)$

- 12.1 Introducción 309
- 12.2 Propiedades de la función gamma 310
- 12.3 Representación integral para la función zeta de Hurwitz 311
- 12.4 Una representación de la función zeta de Hurwitz mediante una integral de contorno 314
- 12.5 La prolongación analítica de la función zeta de Hurwitz 316

- 12.6 Prolongación analítica de $\zeta(s)$ y $L(s, \chi)$ 317
- 12.7 La fórmula de Hurwitz para $\zeta(s, a)$ 318
- 12.8 La ecuación funcional para la función zeta de Riemann 322
- 12.9 Una ecuación funcional para la función zeta de Hurwitz 324
- 12.10 La ecuación funcional para L -funciones 325
- 12.11 Cálculo de $\zeta(-n, a)$ 327
- 12.12 Propiedades de los números de Bernoulli y de los polinómios de Bernoulli 329
- 12.13 Fórmulas para $L(0, \chi)$ 332
- 12.14 Aproximación de $\zeta(s, a)$ por medio de sumas finitas 333
- 12.15 Desigualdades para $|\zeta(s, a)|$ 336
- 12.16 Desigualdades para $|\zeta(s)|$ y para $|L(s, \chi)|$ 338
- Ejercicios del capítulo 12* 339

Capítulo 13

Demostración analítica del teorema del número primo

- 13.1 El plan de la demostración 345
- 13.2 Lemas 347
- 13.3 Una representación de $\psi_1(x)/x^2$ como integral de contorno 351
- 13.4 Cotas superiores para $|\zeta(s)|$ y para $|\zeta'(s)|$ en las proximidades de la recta $\sigma = 1$
- 13.5 La no anulación de $\zeta(s)$ en la recta $\sigma = 1$ 355
- 13.6 Desigualdades para $|1/\zeta(s)|$ y $|\zeta'(s)/\zeta(s)|$ 357
- 13.7 Terminación de la demostración del teorema del número primo 359
- 13.8 Regiones carentes de ceros de $\zeta(s)$ 363
- 13.9 La hipótesis de Riemann 365
- 13.10 Aplicación a la función divisor 366
- 13.11 Aplicación a la indicatriz de Euler 370
- 13.12 Extensión de la desigualdad de Pólya para sumas de caracteres 374
- Ejercicios del capítulo 13* 375

Capítulo 14

Particiones

- 14.1 Introducción 379
- 14.2 Representación geométrica de las particiones 383
- 14.3 Funciones generadoras de particiones 384
- 14.4 El teorema de Euler de los números pentagonales 388
- 14.5 Demostración combinatoria del teorema de los números pentagonales de Euler 391
- 14.6 Fórmula recursiva de Euler para $p(n)$ 394

- 14.7 Una cota superior para $p(n)$ 395
- 14.8 Identidad del triple producto de Jacobi 398
- 14.9 Consecuencias de la identidad de Jacobi 401
- 14.10 Diferenciación logarítmica de funciones generadoras 402
- 14.11 Las identidades de partición de Ramanujan 405
- Ejercicios del capítulo 14* 406

Bibliografía 413

Índice de símbolos especiales 417

Índice alfabético 419

Introducción histórica

La teoría de números es la rama de la Matemática que trata de las propiedades de la totalidad de los números,

1, 2, 3, 4, 5, ...

llamados *números naturales*, o *enteros positivos*.

Los enteros positivos constituyen, sin duda alguna, la primera creación matemática del hombre. Es realmente difícil imaginar los seres humanos sin la habilidad de contar, aunque ésta se hallase reducida a estrechos límites. La Historia nos dice que ya en los años 5700 A.C. los antiguos sumerios disponían de un calendario, luego debían haber desarrollado ya alguna forma de Aritmética.

En los años 2500 A.C. los sumerios desarrollaron un sistema de numeración utilizando 60 como base. Éste pasó a los babilonios que desarrollaron una gran habilidad calculadora. Se han encontrado tablillas de arcilla babilónicas que contienen tablas matemáticas elaboradas, y que se datan en 2000 A.C.

Cuando las antiguas civilizaciones alcanzaron un nivel que les dejaba tiempo libre para pensar sobre las cosas, algunos pueblos empezaron a especular acerca de la naturaleza y propiedades de los números. Esta curiosidad se desarrolló en un cierto misticismo-numérico o «Numerología», y aún hoy números como 3, 7, 11 y 13 se consideran portadores de buena o mala suerte.

Los números se utilizaron para fijar los recuerdos y celebrarlos y para las transacciones comerciales unos 5000 años antes de que se pensase en estudiarlos en sí mismos de forma sistemática. La primera orientación científica al estudio de los enteros, es decir, el origen de la Teoría de los números, se atribuye generalmente a los griegos. Allá por los años 600 A.C., Pitágoras y sus discípulos efectuaron

un estudio bastante completo de los enteros. Fueron los primeros en clasificar los enteros de diversas formas:

Números pares: 2, 4, 6, 8, 10, 12, 14, 16, ...

Números impares: 1, 3, 5, 7, 9, 11, 13, 15, ...

Números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...

Un *número primo* es un número mayor que 1 cuyos únicos divisores son 1 y él mismo. Los números que no son primos se llaman *compuestos*, excepto el número 1 que no se considera ni primo ni compuesto.

Los pitagóricos relacionaron además los números con la Geometría. Introdujeron la idea de *números poligonales*: números triangulares, números cuadráticos, números pentagonales, etc. La razón de esta nomenclatura geométrica aparece clara cuando los números se representan por medio de puntos colocados en forma de triángulos, cuadrados, pentágonos, etc., tal como se indica en la figura 1.1.

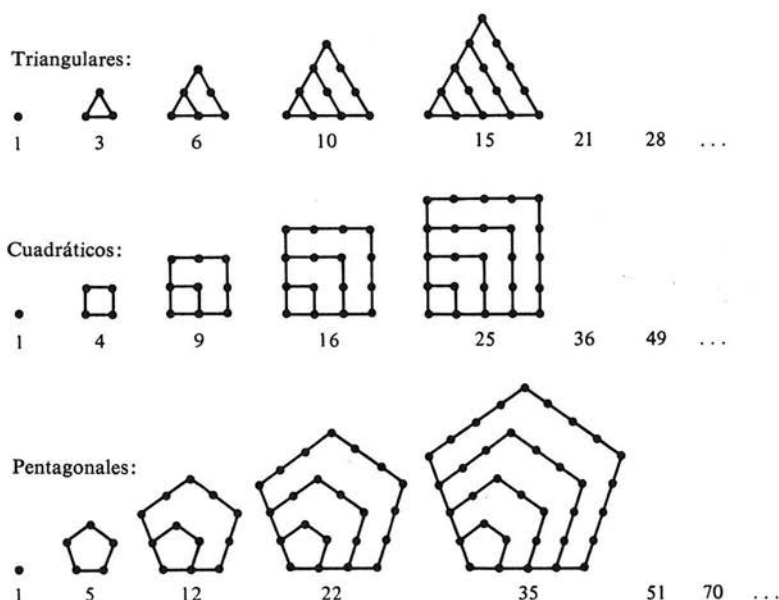


Figura 1.1

Otra conexión con la Geometría procede del famoso teorema de Pitágoras que establece que en todo triángulo rectángulo el cuadrado de la longitud de la hipotenusa es igual a la suma de los cuadrados de las longitudes de los catetos (ver figura

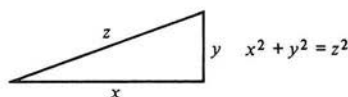


Figura 1.2

ra 1.2). Los pitagóricos se interesaron por los triángulos rectángulos cuyos lados eran enteros, como los de la figura 1.3. Tales triángulos se conocen como *triángulos pitagóricos*. La correspondiente terna de números (x, y, z) que representan las longitudes de los lados se llama *terna pitagórica*.

Se ha encontrado una tablilla babilónica, datada alrededor de 1700 A.C., que contiene una lista extensa de ternas pitagóricas, algunos de cuyos números son bastante grandes. Los pitagóricos fueron los primeros en proporcionar un método para determinar infinitudes de ternas. En notación moderna podemos describirlo como sigue: Sea n un número impar mayor que 1, y sea

$$x = n, \quad y = \frac{1}{2}(n^2 - 1), \quad z = \frac{1}{2}(n^2 + 1).$$

La terna que resulta (x, y, z) constituye siempre una terna pitagórica con $z = y + 1$. He aquí algunos ejemplos:

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

Además de éstas existen otras ternas pitagóricas; por ejemplo:

x	8	12	16	20
y	15	35	63	99
z	17	37	65	101

En estos ejemplos tenemos $z = y + 2$. Platón (430-349 A.C.) justificó un método para determinar todas estas ternas; en notación moderna viene dado por las fórmulas

$$x = 4n, \quad y = 4n^2 - 1, \quad z = 4n^2 + 1.$$

Alrededor de 300 A.C. ocurrió, en la historia de la Matemática, un suceso realmente importante. La aparición de los *Elementos* de Euclides, una colección de 13 libros, transformó las matemáticas de la Numerología en una ciencia deductiva. Euclides fue el primero en presentar hechos matemáticos junto con demostraciones rigurosas de tales hechos.

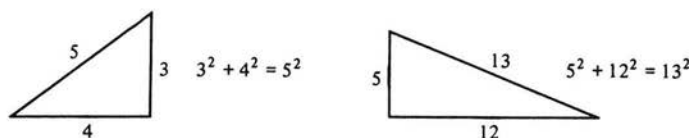


Figura I.3

Tres de tales libros se hallan dedicados a la Teoría de números (Libros VII, IX y X). En el libro IX Euclides demostró que existe una infinidad de números primos. Esta demostración todavía se enseña hoy en nuestras aulas. En el libro X dio un método para obtener todas las ternas pitagóricas si bien no demuestra que este método, realmente, las da todas. El método se puede establecer sumariamente por las fórmulas

$$x = t(a^2 - b^2), \quad y = 2tab, \quad z = t(a^2 + b^2),$$

en donde t , a , y b , son enteros positivos arbitrarios tales que $a > b$, a y b carecen de factores primos comunes, y uno de ellos, a ó b , es par y el otro impar.

Además Euclides aportó una importante contribución a otro problema planteado por los pitagóricos —el de buscar todos los números perfectos. El número 6 fue llamado número perfecto puesto que $6 = 1 + 2 + 3$, que es la suma de sus divisores propios (esto es, la suma de todos los divisores menores que 6). Otro ejemplo de número perfecto es 28 puesto que $28 = 1 + 2 + 4 + 7 + 14$, y 1, 2, 4, 7, y 14 son los divisores de 28 menores que 28. Los griegos se referían a los divisores propios de un número llamándolos sus «partes». Los números 6 y 28 se llamaron perfectos porque eran iguales a la suma de todas sus partes.

En el libro IX Euclides da todos los números perfectos *pares*. Demuestra que un número par es perfecto si tiene la forma

$$2^{p-1}(2^p - 1),$$

en donde p y $2^p - 1$ son primos.

Dos mil años más tarde, Euler demostró el recíproco del teorema de Euclides. Esto es, cada número perfecto par debe ser del tipo descrito por Euclides. Por ejemplo, para 6 y 28 tenemos

$$6 = 2^{2-1}(2^2 - 1) = 2 \cdot 3 \quad \text{y} \quad 28 = 2^{3-1}(2^3 - 1) = 4 \cdot 7.$$

Los cinco primeros números pares perfectos son

$$6, 28, 496, 8128 \quad \text{y} \quad 33\,550\,336.$$

Los números perfectos son, realmente, muy raros. En el momento actual (1980) sólo se conocen 24 números perfectos. Corresponden a los siguientes valores de p en la fórmula de Euclides:

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, \\ 3217, 4253, 4423, 9689, 9941, 11213, 19937.$$

Los números de la forma $2^p - 1$, en donde p es primo, se conocen con el nombre de *números de Mersenne* y se designan por M_p en honor de Mersenne, que los estudió en 1644. Se sabe que M_p es primo para los 24 primos dados en la lista anterior y compuesto para todos los demás valores de $p \leq 257$, excepto quizás para

$$p = 157, 167, 193, 199, 227, 229;$$

para éstos no se sabe si M_p es primo o compuesto.

No se conoce ningún número perfecto *impar*; tampoco se sabe si existen. Pero si existen deben ser muy grandes; de hecho, mayores que 10^{50} (ver Hagis [29]).

Ahora volvemos a una breve descripción histórica de la Teoría de números desde el tiempo de Euclides.

Después de Euclides, 300 A.C., no se efectuaron avances significativos en Teoría de números hasta aproximadamente 250 D.C. en que otro matemático griego, Diofanto de Alejandría, publicó 13 libros, de los que se han conservado seis. Esta es la primera obra griega en la que se realiza un uso sistemático de los símbolos algebraicos. Si bien dicha notación algebraica parece torpe frente a la usual de hoy día, Diofanto fue hábil para resolver ecuaciones algebraicas con dos o tres incógnitas. Muchos de estos problemas se originaron en la Teoría de números y a él le pareció natural buscar soluciones *enteras* para las ecuaciones. Las ecuaciones que deben ser resueltas por medio de valores enteros de las incógnitas se llaman hoy *ecuaciones diofánticas*, y el estudio de tales ecuaciones recibe el nombre de *Análisis diofántico*. La ecuación $x^2 + y^2 = z^2$ relativas a las ternas pitagóricas constituye un ejemplo de ecuación diofántica.

Tras Diofanto no se realizaron muchos progresos en Teoría de números hasta el siglo diecisiete, si bien existe evidencia de que el tema empezaba a florecer en el Lejano Oriente —especialmente en la India— en el período entre 500 D.C. y 1200 D.C.

En el siglo diecisiete el tema renació en la Europa Oeste, en gran manera gracias a los esfuerzos de un matemático francés, Pierre de Fermat (1601-1665), que se conoce generalmente como el padre de la Teoría moderna de números. Gran parte de la inspiración de Fermat deriva de los trabajos de Diofanto. Fue el primero en descubrir propiedades realmente profundas de los enteros. Fermat demostró los siguientes teoremas sorprendentes:

Todo entero o es un número triangular o una suma de 2 o 3 números triangulares; todo entero o es cuadrático o es una suma de 2, 3 o 4 cuadráticos; todo entero es pentagonal o es una suma de 2, 3, 4 ó 5 números pentagonales, y así sucesivamente.

Fermat descubrió también que todo número primo de la forma $4n + 1$ tal como 5, 13, 17, 29, 37, 41, etc., es una suma de dos cuadrados. Por ejemplo,

$$\begin{array}{llll} 5 = 1^2 + 2^2, & 13 = 2^2 + 3^2, & 17 = 1^2 + 4^2, & 29 = 2^2 + 5^2, \\ & 37 = 1^2 + 6^2, & 41 = 4^2 + 5^2. & \end{array}$$

Poco tiempo después de Fermat, los nombres de Euler (1707-1783), Lagrange (1763-1813), Legendre (1752-1833), Gauss (1777-1855), y Dirichlet (1805-1859) resultaron prominentes en el posterior desarrollo de la teoría. El primer libro de Teoría de números fue publicado por Legendre en 1798. Tres años más tarde Gauss publicó *Disquisitiones Arithmeticae*, un libro que transformaba la materia en una ciencia sistemática y bella. Sin embargo utilizaba gran cantidad de contribuciones de otras ramas de la Matemática, así como de otras ciencias. El mismo Gauss consideraba este libro sobre Teoría de números su mejor obra.

En los últimos doscientos años, o sea desde los tiempos de Gauss, ha existido un desarrollo intenso de la materia en muchas direcciones. Es imposible dar en pocas páginas una clara exposición de los tipos de problemas que se estudian en la Teoría de números. El campo es muy vasto y algunas de sus partes requieren un profundo conocimiento de matemáticas superiores. A pesar de todo, existen muchos problemas de Teoría de números que resulta muy fácil enunciarlos. Algunos de ellos se refieren a números primos, y dedicamos el resto de esta introducción a tales problemas.

En las páginas anteriores hemos dado la lista de los primos menores que 100. Una tabla que daba la lista de todos los números primos menores que 10 millones fue publicada en 1914 por un matemático americano, D. N. Lehmer [43]. Existen exactamente 664 579 primos menores que 10 millones, o aproximadamente $6\frac{1}{2}\%$. Más recientemente D. H. Lehmer (el hijo de D. N. Lehmer) calculó el total de primos menores que 10 mil millones; hay exactamente 455 052 512 de tales primos, o sea aproximadamente $4\frac{1}{2}\%$ si bien no se conocen todos estos primos individualmente (ver Lehmer [41]).

Un examen detallado de una tabla de primos pone de manifiesto que se hallan distribuidos de forma muy irregular. Las tablas muestran grandes espacios entre

primos. Por ejemplo, el primo 370 261 va seguido de 111 compuestos. No existe primo alguno entre 20 831 323 y 20 831 533. Es fácil demostrar que entre números primos se pueden presentar eventualmente espacios arbitrariamente grandes.

Por otro lado, las tablas muestran que se presentan reiteradamente primos consecutivos tales como 3 y 5, o 101 y 103. Los primos que, como éstos, difieren sólo en dos unidades se conocen como *primos gemelos*. Hay unos 1000 pares gemelos por debajo de 100 000 y unos 8000 por debajo de 1 000 000. El par más grande conocido hoy por hoy (ver Williams y Zarnke [76]) es $76 \cdot 3^{139} - 1$ y $76 \cdot 3^{139} + 1$. Muchos matemáticos creen que existe una infinidad de estos pares, pero ninguno ha sido capaz de demostrarlo.

Una de las razones de la irregularidad en la distribución de primos es que no existe ninguna fórmula simple que produzca todos los números primos. Algunas fórmulas proporcionan muchos primos. Por ejemplo, la expresión

$$x^2 - x + 41$$

da un primo para $x = 0, 1, 2, \dots, 40$, mientras que

$$x^2 - 79x + 1601$$

da un primo para $x = 0, 1, 2, \dots, 79$. Sin embargo, ninguna de tales fórmulas simples puede dar un primo para todo x , aunque se utilicen cubos y potencias superiores. De hecho, en 1752 Goldbach probó que ningún polinomio en x con coeficientes enteros puede ser primo para todo x , e incluso para x suficientemente grande.

Algunos polinomios representan infinidad de primos. Por ejemplo, cuando x , recorre los enteros $0, 1, 2, 3, \dots$, el polinomio lineal

$$2x + 1$$

da todos los números impares por lo tanto una infinidad de primos. También, cada uno de los polinomios

$$4x + 1 \quad \text{y} \quad 4x + 3$$

representa una infinidad de primos. En un trabajo famoso [15] publicado en 1837, Dirichlet demostró que, si a y b son enteros positivos carentes de factores comunes, el polinomio

$$ax + b$$

da una infinidad de primos cuando x recorre todos los enteros positivos. Este resultado se conoce como teorema de Dirichlet sobre la existencia de primos en una progresión aritmética dada.

Para demostrar el teorema, Dirichet salió fuera del reino de los enteros e introdujo instrumentos de Análisis tales como los límites y la continuidad. Por este motivo puso los fundamentos de una nueva rama de la Matemática llamada *Teoría analítica de números*, en la cual se utilizan ideas y métodos del Análisis real y complejo para resolver problemas sobre enteros.

No se sabe si existe un polinomio cuadrático $ax^2 + bx + c$ con $a \neq 0$ que representa una infinidad de primos. Sin embargo, Dirichley [16] utilizó sus poderosos métodos analíticos para demostrar que, si a , $2b$, y c carecían de factores primos comunes, el polinomio cuadrático en dos variables

$$ax^2 + 2bxy + cy^2$$

representa una infinidad de primos cuando x e y recorren los enteros positivos.

Fermat creía que la fórmula $2^{2^n} + 1$ daría siempre un primo para $n = 0, 1, 2, \dots$. Estos números se llaman *números de Fermat* y se designan por F_n . Los cinco primeros son:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \quad \text{y} \quad F_4 = 65\,537,$$

y todos ellos son primos. Sin embargo, en 1732 Euler halló que F_5 es compuesto; de hecho

$$F_5 = 2^{32} + 1 = (641)(6\,700\,417).$$

Estos números son de interés también en Geometría plana. Gauss demostró que, si F_n es un primo, por ejemplo $F_n = p$, entonces se puede construir un polígono regular de p lados con regla y compás.

Más allá de F_5 no se han hallado otros primos de Fermat. En efecto, para $5 \leq n \leq 16$, cada número de Fermat F_n es compuesto. Además, se sabe que F_n es compuesto para los siguientes valores aislados de n :

$$n = 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, \\ 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, \\ \text{y } 1945.$$

El mayor número de Fermat compuesto, F_{1945} , tiene más de 10^{582} dígitos, un número mayor que el número de letras de los listines telefónicos de Los Angeles y New York juntos (ver Robinson [59] y Wrathall [77]).

Ya hemos mencionado anteriormente que no existe ninguna fórmula simple que dé todos los primos. En conexión con este hecho, mencionemos un resultado descubierto en 1947 por un matemático americano, W. H. Mills [50]. Demostro que existe algún número A , mayor que 1 pero no entero tal que

$$[A^{3^x}] \text{ es primo para todo } x = 1, 2, 3, \dots$$

Aquí $[A^{3^x}]$ significa el mayor entero $\leq A^{3^x}$. Por desgracia se desconoce a qué es igual A .

Los resultados anteriores ilustran la irregularidad de la distribución de los números primos. Sin embargo, si se examinan grandes bloques de primos se encuentra que su distribución media parece bastante regular. Si bien no se terminan los números primos, se presentan cada vez más espaciados, en media, a medida que se avanza en la tabla. La cuestión del enrarecimiento en la distribución fue motivo de muchas especulaciones en el siglo diecinueve. Para estudiar esta distribución, consideramos una función, designada por $\pi(x)$, que cuenta el número de primos $\leq x$. Luego

$$\pi(x) = \text{al número de primos } p \text{ que verifican } 2 \leq p \leq x.$$

A continuación se da una breve tabla de esta función y su comparación con $x/\log x$, en donde $\log x$ es el logaritmo neperiano de x .

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$
10	4	4,3	0,93
10^2	25	21,7	1,15
10^3	168	144,9	1,16
10^4	1 229	1 086	1,11
10^5	9 592	8 686	1,10
10^6	78 498	72 464	1,08
10^7	664 579	621 118	1,07
10^8	5 761 455	5 434 780	1,06
10^9	50 847 534	48 309 180	1,05
10^{10}	455 052 512	434 294 482	1,048

Examinando una tabla como ésta para $x \leq 10^6$, Gauss [24] y Legendre [40] propusieron independientemente que, para x grande, el cociente

$$\pi(x) / \frac{x}{\log x}$$

era próximo a 1 y conjeturaron que este cociente tendía a 1 cuando x tendía a ∞ . Tanto Gauss como Legendre intentaron demostrar esta afirmación pero no tuvieron éxito. El problema de determinar la veracidad o falsedad de esta conjetura atrajo la atención de matemáticos eminentes durante cerca de 100 años.

En 1851 el matemático ruso Chebyshev [9] dio un paso importante al demostrar que *si* dicho cociente tenía límite, este límite debía ser 1. Sin embargo no fue capaz de demostrar que el cociente *tenía* límite.

En 1859 Riemann [58] atacó el problema con métodos analíticos, utilizando una fórmula descubierta por Euler en 1737 que relaciona los números primos con la función

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

para s real > 1 . Riemann consideró valores complejos de s y dio un método ingenioso para conectar la distribución de los primos con las propiedades de la función $\zeta(s)$. Las matemáticas necesarias para justificar todos los detalles de este método no habían sido desarrolladas completamente y Riemann no fue capaz de resolver completamente el problema anterior antes de su muerte en 1866.

Treinta años más tarde se establecieron las herramientas analíticas necesarias y en 1896 J. Hadamard [28] y C. J. de la Vallée Poussin [71] demostraron, independientemente y casi simultáneamente, que

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

Este resultado notable se llama el *teorema del número primo*, y su demostración constituyó uno de los éxitos más completos de la Teoría analítica de números.

En 1949, dos matemáticos contemporáneos, Atle Selberg [62] y Paul Erdős [19] causaron sensación en el mundo matemático al descubrir una demostración elemental del teorema del número primo. Su demostración, si bien es muy intrincada no utiliza ni $\zeta(s)$ ni la teoría de las funciones complejas y, en principio, es accesible a todo el que se halle familiarizado con el Cálculo elemental.

Uno de los problemas más famosos relativos a números primos lo constituye la llamada *conjetura de Goldbach*. En 1742, Goldbach [26] escribió a Euler sugiriéndole que cada número par ≥ 4 es una suma de dos primos. Por ejemplo,

$$\begin{array}{lll} 4 = 2 + 2, & 6 = 3 + 3, & 8 = 3 + 5, \\ 10 = 3 + 7 = 5 + 5, & 12 = 5 + 7. \end{array}$$

Esta conjetura está sin decidir hasta hoy, si bien en los últimos años se han efectuado ciertos progresos que indican que probablemente es verdadera. ¿Por qué los matemáticos piensan actualmente que *probablemente* es verdadera si no han sido capaces de demostrarla? Ante todo, la conjetura ha sido comprobada por computación efectiva para todo número par menor que 33×10^6 . Se ha establecido que cada número par mayor que 6 y menor que 33×10^6 es, en efecto, no sólo la suma de dos primos impares sino la suma de dos primos impares *distintos* (ver Shen [66]). Pero en Teoría de números la comprobación de unos pocos centenares de casos no constituye evidencia suficiente para convencer a los matemáticos de que algo es *probablemente* verdadero. Por ejemplo, todos los primos impares se dividen en dos categorías, los de la forma $4n + 1$ y los de la forma $4n + 3$. Sea $\pi_1(x)$ la notación de todos los primos $\neq x$ que son de la forma $4n + 1$, y sea $\pi_3(x)$ la de los números que son de la forma $4n + 3$. Sabemos que existe una infinidad de primos de ambos tipos. Por computación se estableció que $\pi_1(x) \neq \pi_3(x)$ para todo $x < 26\,861$. Pero en 1957, J. Leech [39] estableció que para $x = 26\,861$ se verificaba $\pi_1(x) = 1473$ y $\pi_3(x) = 1472$, luego la desigualdad se invertía. En 1914, Littlewood [49] demostró que con una frecuencia infinita esta desigualdad se invertía de sentido. Esto es, existe una infinidad de x para los que $\pi_1(x) \leq \pi_3(x)$ y también una infinidad de x para los que $\pi_3(x) \leq \pi_1(x)$. Las conjeturas relativas a los números primos pueden ser erróneas a pesar de haber sido comprobadas por el cálculo de centenares de casos.

Por consiguiente, el hecho de que la conjetura de Goldbach se haya verificado para todos los números pares menores que 33×10^6 constituye únicamente un poco de evidencia a su favor.

Otra forma que tienen los matemáticos para evidenciar la veracidad de una conjetura particular consiste en demostrar otros teoremas que son algo parecidos a la conjetura. Por ejemplo, en 1930 el matemático ruso Schnirelmann [61] demostró que existe un M tal que cada n , a partir de un lugar, es una suma de M o menos primos:

$$n = p_1 + p_2 + \cdots + p_M \quad (\text{para } n \text{ suficientemente grande})$$

Si supiésemos que M es igual a 2 para todo n par, habríamos demostrado la conjetura de Goldbach para n suficientemente grande. En 1956 el matemático chino Yin Wen-Lin [78] demostró que $M \leq 18$. Esto es, cada número n , a partir de un lugar, es suma de 18 o menos primos. El resultado de Schnirelmann se considera un paso de gigante con vistas a demostrar la conjetura de Goldbach. Es el primer progreso real efectuado en este problema en casi 200 años.

Un planteamiento más preciso a la solución del problema de Goldbach fue establecido en 1937 por otro matemático ruso, I. M. Vinogradov [73], el cual demostró que, a partir de un lugar, todo número *impar* es la suma de *tres* primos:

$$n = p_1 + p_2 + p_3 \quad (n \text{ impar, } n \text{ suficientemente grande}).$$

De hecho, este resultado es verdadero para todo n impar mayor que 3^{31} (ver Borodzikin [5]). Hoy constituye la pieza más importante de evidencia en favor de la conjetura de Goldbach. Por un lado, es fácil demostrar que el teorema de Vinogradov es una consecuencia de la afirmación de Goldbach. Es decir, si la conjetura de Goldbach es verdadera, entonces la afirmación de Vinogradov se deduce fácilmente. La conquista más sobresaliente de Vinogradov fue su habilidad para probar su resultado sin utilizar la conjetura de Goldbach. Por desgracia, nadie ha sido capaz de establecerlo en el otro sentido y de demostrar la afirmación de Goldbach a partir de la de Vinogradov.

Otra pieza de la evidencia en favor de la conjetura de Goldbach fue establecida en 1948 por el matemático húngaro Rényi [57] que demostró que existe un número M tal que cada número impar n suficientemente grande se puede escribir como suma de un primo con otro número que no posee más de M factores primos:

$$n = p + A,$$

en donde A no posee más de M factores primos (n par, n suficientemente grande). Si supiésemos que $M = 1$ entonces la conjetura de Goldbach sería cierta para todo n suficientemente grande. En 1965 A. A. Buhstab [6] y A. I. Vinogradov [72] demostraron que $M \leq 3$, y en 1966 Chen Jing-run [10] demostró que $M \leq 2$.

Concluimos esta introducción con una breve mención de algunos de los problemas no resueltos concernientes a números primos.

1. (Problema de Goldbach). ¿Existe un número par > 2 que no sea suma de dos primos?
2. ¿Existe un número par > 2 que no sea la diferencia de dos primos?
3. ¿Existe una infinidad de primos gemelos?
4. ¿Existe una infinidad de primos de Mersenne, esto es, primos de la forma $2^p - 1$, p primo?
5. ¿Existe una infinidad de números compuestos de Mersenne?
6. ¿Existe una infinidad de primos de Fermat, esto es, primos de la forma $2^{2^n} + 1$?
7. ¿Existe una infinidad de números de Fermat compuestos?
8. ¿Existe una infinidad de primos de la forma $x^2 + 1$, en donde x es un entero? (Sabemos que existe una infinidad de primos de la forma $x^2 + y^2$, y de la forma $x^2 + y^2 + 1$, y de la forma $x^2 + y^2 + z^2 + 1$).
9. ¿Existe una infinidad de primos de la forma $x^2 + k$ (k dado)?

10. ¿Existe siempre un primo, por lo menos, entre n^2 y $(n+1)^2$ para cada entero $n \geq 1$?
11. ¿Existe siempre un primo, por lo menos, entre n^2 y $n^2 + n$ para cada entero $n > 1$?
12. ¿Existe una infinidad de primos cuyos dígitos (en base 10) son todos unos? (Existen dos ejemplos: 11 y 11 111 111 111 111 111 111 111.)

El matemático profesional se siente atraído por la Teoría de números porque en sus métodos se pueden utilizar todas las armas de la Matemática moderna para esclarecer sus problemas. Es una realidad que ramas muy importantes de la Matemática han tenido su origen en la Teoría de números. Por ejemplo, los primeros intentos para resolver el teorema del número primo estimularon el desarrollo de la teoría de las funciones complejas, especialmente la teoría de las funciones enteras. Los intentos para demostrar que la ecuación diofántica $x^n + y^n + z^n$ no posee soluciones no triviales si $n \geq 3$ (conjetura de Fermat) contribuyeron al desarrollo de la Teoría algebraica de números, una de las áreas más activas de la investigación matemática actual. Si bien la conjetura de Fermat permanece sin decidir, ello parece poco importante frente a la gran cantidad de teorías matemáticas que han sido creadas como resultado de los trabajos acerca de dicha conjetura. Otro ejemplo lo constituye la teoría de las particiones que ha constituido un factor importante en el desarrollo del Análisis combinatorio y en el estudio de las funciones modulares.

Existen centenares de problemas no resueltos en Teoría de números. Aparecen problemas nuevos más rápidamente que se resuelven los antiguos, y muchos de los antiguos llevan siglos sin resolverse. Como dijo una vez el matemático Sierpinski, «...el progreso de nuestro conocimiento de los números avanza no sólo por lo que de ellos ya conocemos, sino también porque nos damos cuenta de lo que todavía de ellos desconocemos».

Nota. Todo estudiante serio de Teoría de números ha de estar familiarizado con los tres volúmenes de la obra de Dickson, *History of the Theory of Numbers* [13], y con los seis volúmenes de la de Le Veque, *Reviews in Number Theory* [45]. La *History* de Dickson proporciona un conocimiento enciclopédico de toda la literatura de la Teoría de números hasta 1918. Los volúmenes de Le Veque reproducen todos los artículos de los volúmenes 1-44 de las *Mathematical Reviews* (1940-1972) que se refieren directamente a cuestiones consideradas comúnmente como parte de la Teoría de números. Estas dos valiosas colecciones proporcionan prácticamente una historia de todos los descubrimientos importantes en Teoría de números desde la antigüedad hasta 1972.

Capítulo 1

El teorema fundamental de la Aritmética

1.1 INTRODUCCIÓN

En este capítulo se introducen conceptos básicos de la Teoría elemental de números tales como la divisibilidad, el máximo común divisor, y los números primos y compuestos. Los resultados principales son el teorema 1.2, que establece la existencia del máximo común divisor para todo par de enteros, y el teorema 1.10, (el teorema fundamental de la Aritmética), que demuestra que todo entero mayor que 1 se puede representar como producto de factores primos de forma única (salvo el orden de los factores). Muchas de las demostraciones utilizan la siguiente propiedad de los enteros.

El principio de inducción. *Si Q es un conjunto de enteros tales que*

- (a) $1 \in Q$,
- (b) $n \in Q$ implica $n + 1 \in Q$,

entonces

- (c) *todo entero ≥ 1 pertenece a Q .*

Existen, además, otras formulaciones de este principio. Por ejemplo, en (a) podemos substituir 1 por un entero cualquiera k , siempre que en (c) la desigualdad ≥ 1 se substituya por $\geq k$. Además (b) se puede substituir por 1, 2, 3, ..., $n \in Q$ implica $(n + 1) \in Q$.

Suponemos que el lector se halla familiarizado con este principio así como con su uso en las demostraciones de teoremas por inducción. Le suponemos también familiarizado con el siguiente principio que es lógicamente equivalente al principio de inducción.

El principio de buena ordenación. Si A es un conjunto no vacío de enteros positivos, entonces A posee un elemento mínimo.

De nuevo, este principio posee formulaciones equivalentes. Por ejemplo, «enteros positivos» se puede substituir por «enteros $\geq k$ para un cierto k ».

1.2 DIVISIBILIDAD

Notación. En este capítulo, las letras latinas minúsculas a, b, c, d, n , etc., denotan enteros; pueden ser positivos, negativos, o cero.

Definición de divisibilidad. Diremos que d divide n y escribiremos $d|n$ si $n = cd$ para un c . Diremos también que n es un múltiplo de d , que d es un divisor de n , o que d es un factor de n . Si d no divide a n escribiremos $d \nmid n$.

La divisibilidad establece una relación binaria entre enteros con las siguientes propiedades elementales cuyas demostraciones se dejan como ejercicio para el lector, (Salvo indicación expresa, las letras a, b, d, m, n del teorema 1.1 representan enteros arbitrarios.)

Teorema 1.1 La divisibilidad verifica las siguientes propiedades:

- | | |
|---|--------------------------------|
| (a) $n n$ | (propiedad reflexiva) |
| (d) $d n$ y $n m$ implica $d m$ | (propiedad transitiva) |
| (c) $d n$ y $d m$ implica $d (an + bm)$ | (propiedad lineal) |
| (d) $d n$ implica $ad an$ | (propiedad de multiplicación) |
| (e) $ad an$ y $a \neq 0$ implica $d n$ | (propiedad de simplificación) |
| (f) $1 n$ | (1 divide a todos los enteros) |
| (g) $n 0$ | (cada entero divide a cero) |
| (h) $0 n$ implica $n = 0$ | (el cero sólo divide al cero) |
| (i) $d n$ y $n \neq 0$ implica $ d \leq n $ | (propiedad de comparación) |
| (j) $d n$ y $n d$ implica $ d = n $ | |
| (k) $d n$ y $d \neq 0$ implica $(n/d) n$. | |

Nota. Si $d|n$ entonces n/d se llama el divisor conjugado de d .

1.3 MÁXIMO COMÚN DIVISOR

Si un d divide a dos enteros a y b , entonces d se llama *divisor común* de a y b . Así, pues, 1 es un divisor común de todo par de enteros a y b . Ahora demostraremos que todo par de enteros a y b poseen un divisor común que se puede expresar como combinación lineal de a y b .

Teorema 1.2 *Dados dos enteros a y b , existe un divisor común de a y b de la forma*

$$d = ax + by,$$

en donde x e y son enteros. Además, todo divisor común de a y b divide a este d .

DEMOSTRACIÓN. Ante todo suponemos que $a \geq 0$ y $b \geq 0$. Utilizamos inducción sobre n , en donde $n = a + b$. Si $n = 0$ entonces $a = b = 0$ y podemos tomar $d = 0$ con $x = y = 0$. Podemos pues suponer que el teorema se ha demostrado para $0, 1, 2, \dots, n-1$. Por simetría podemos suponer que $a \geq b$. Si $b = 0$ tomamos $d = a$, $x = 1$, $y = 0$. Si $b \geq 1$ aplicamos el teorema a $a-b$ y b . Puesto que $(a-b) + b = a = n-b \leq n-1$, la hipótesis de inducción es aplicable y existe un divisor común d de $a-b$ y b de la forma $d = (a-b)x + by$. Este d divide también a $(a-b) + b = a$, luego d es un divisor común de a y b y se tiene $d = ax + (y-x)b$, como combinación lineal de a y b . Para completar la demostración necesitamos demostrar que cada divisor común divide a d . Pero un divisor común divide a a y a b y por lo tanto, por linealidad, divide a d .

Si $a < 0$ o $b < 0$ (o ambos), podemos aplicar el resultado recién demostrado a $|a|$ y $|b|$. Entonces existe un divisor común d de $|a|$ y $|b|$ de la forma

$$d = |a|x + |b|y.$$

Si $a < 0$, $|a|x = -ax = -a(-x)$. Análogamente, si $b < 0$, $|b|y = b(-y)$. Por lo tanto d es también ahora combinación lineal de a y b . $\square$

Teorema 1.3 *Dados dos enteros a y b , existe un número d y sólo uno, con las siguientes propiedades:*

- | | |
|---------------------------------|---|
| (a) $d \geq 0$ | (d es no negativo) |
| (b) $d a$ y $d b$ | (d es un divisor común de a y de b) |
| (c) $e a$ y $e b$ implica $e d$ | (cada divisor común divide a d). |

DEMOSTRACIÓN. Por el teorema 1.2 por lo menos existe un d que satisface las condiciones (b) y (c). Luego, $-d$ también las satisface. Pero si d' satisface (b) y (c), entonces $d|d'$ y $d'|d$, por lo tanto $|d| = |d'|$. Luego existe exactamente un $d \geq 0$ que satisface (b) y (c). $\square$

Nota. En el teorema 1.3, $d = 0$ si, y sólo si, $a = b = 0$. En cualquier otro caso $d \geq 1$.

Definición. El número d del teorema 1.3 se llama máximo común divisor (mcd) de a y b y se designa por (a, b) o aDb . Si $(a, b) = 1$ entonces se dice que a y b son primos entre sí (o relativos).

La notación aDb surge al interpretar el mcd como una operación entre a y b . Sin embargo, la notación más comúnmente usada es (a, b) y es la que adoptaremos, si bien en el próximo teorema utilizaremos también la notación aDb con objeto de hacer resaltar las propiedades algebraicas de la operación D .

Teorema 1.4 *El mcd posee las siguientes propiedades:*

- (a) $(a, b) = (b, a)$
 $aDb = bDa$ (ley conmutativa)
- (b) $(a, (b, c)) = ((a, b), c)$
 $aD(bDc) = (aDb)Dc$ (ley asociativa)
- (c) $(ac, bc) = |c|(a, b)$
 $(ca)D(cb) = |c|(aDb)$ (ley distributiva)
- (d) $(a, 1) = (1, a) = 1$, $(a, 0) = (0, a) = |a|$.
 $aD1 = 1Da = 1$, $aD0 = 0Da = |a|$.

DEMOSTRACIÓN. Solamente demostraremos (c). Las otras demostraciones se dejan como ejercicio para el lector.

Sea $d = (a, b)$ y sea $e = (ac, bc)$. Queremos demostrar que $e = |c|d$. Escribimos $d = ax + by$. Entonces tenemos

$$(1) \quad cd = acx + bcy.$$

Por lo tanto $cd|e$ puesto que cd divide a ac y bc . Además, la ecuación (1) prueba que $e|cd$ puesto que $e|ac$ y $e|bc$. Por lo tanto $|e| = |cd|$, o $e = |c|d$. $\square$

Teorema 1.5 Lema de Euclides. Si $a|bc$ y si $(a, b) = 1$, entonces $a|c$.

DEMOSTRACIÓN. Puesto que $(a, b) = 1$ podemos escribir $1 = ax + by$. Por consiguiente $c = acx + bcy$. Pero $a|acx$ y $a|bcy$, luego $a|c$. $\square$

1.4 NÚMEROS PRIMOS

Definición. Un entero n se llama primo si $n > 1$ y si los únicos divisores positivos de n son 1 y n . Si $n > 1$ y n no es primo, entonces n se llama compuesto.

EJEMPLOS. Los números primos menores que 100 son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Notación. Los números primos usualmente se designan por p, p', p_i, q, q', q_i .

Teorema 1.6 *Cada entero $n > 1$ o es primo o es producto de números primos.*

DEMOSTRACIÓN. Utilizaremos inducción sobre n . El teorema es claro para $n = 2$. Suponemos que es cierto para cada entero $< n$. Entonces si n no es primo posee un divisor $d \neq 1, d \neq n$. Por lo tanto $n = cd$, en donde $c \neq n$. Luego tanto c como d son $< n$ y < 1 , por lo que cada uno de ellos es un producto de números primos, y entonces n también lo es. $\square$

Teorema 1.7 *Euclides. Existe una infinidad de números primos.*

DEMOSTRACIÓN DE EUCLIDES. Suponemos que sólo existe un número finito, por ejemplo $p_1, p_2, \dots, p_n$. Sea $N = 1 + p_1 p_2 \dots p_n$. Puesto que $N > 1$ o N es primo o N es un producto de primos. Pero N no es primo ya que N es mayor que cada uno de los p_i . Sin embargo ningún p_i divide a N (si $p_i|N$ entonces p_i divide la diferencia $N - p_1 p_2 \dots p_n = 1$). Lo que contradice el teorema 1.6. $\square$

Teorema 1.8 *Si un primo p no divide a a , entonces $(p, a) = 1$.*

DEMOSTRACIÓN. Sea $d = (p, a)$. Entonces $d|p$, luego o $d = 1$ o $d = p$. Pero $d|a$ luego $d \neq p$ puesto que $p \nmid a$. En consecuencia $d = 1$. $\square$

Teorema 1.9 *Si un primo p divide a ab , entonces $p|a$ ó $p|b$. En general, si un primo p divide a un producto $a_1 \dots a_n$, entonces p divide a uno, por lo menos, de los factores.*

DEMOSTRACIÓN. Suponemos que $p|ab$ y que $p \nmid a$. Veremos que $p|b$. Por el teorema 1.8, $(p, a) = 1$, luego por el lema de Euclides, $p|b$.

Para demostrar la afirmación más general se emplea la inducción sobre n , número de factores. Los detalles se dejan al lector. $\square$

1.5 EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

Teorema 1.10 Teorema fundamental de la Aritmética. *Cada entero $n > 1$ se puede representar como un producto de factores primos de forma única, salvo el orden de los factores.*

DEMOSTRACIÓN. Usaremos la inducción sobre n . El teorema es verdadero para $n = 2$. Suponemos, entonces, que es verdadero para todo entero mayor que 1 y menor que n . Probaremos que es verdadero también para n . Si n es primo no hay que probar nada. Por lo tanto, suponemos que n es compuesto y admite dos descomposiciones, que son

$$(2) \quad n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t.$$

Queremos demostrar que $s = t$ y que cada p es igual a algún q . Dado que p_1 divide el producto $q_1 q_2 \cdots q_t$ debe dividir a uno, por lo menos, de los factores. Ordenaremos los $q_1, q_2, \dots, q_t$ de forma que $p_1 | q_1$. Entonces $p_1 = q_1$ ya que p_1 y q_1 son primos. En (2) podemos dividir por p_1 obteniendo

$$n/p_1 = p_2 \cdots p_s = q_2 \cdots q_t.$$

Si $s > 1$ o $t > 1$, entonces $1 < n/p_1 < n$. La hipótesis de inducción nos dice que las dos descomposiciones de n/p_1 son idénticas, si prescindimos del orden de los factores. Por consiguiente $s = t$ y las descomposiciones de (2) son también idénticas, si prescindimos del orden de los factores. Esto completa la demostración. $\square$

Nota. En la descomposición de un entero n , un cierto primo p puede aparecer más de una vez. Si los factores primos *distintos* de n son $p_1, \dots, p_r$ y si p_i aparece a_i veces como factor, escribiremos

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

o más brevemente,

$$n = \prod_{i=1}^r p_i^{a_i}.$$

Esta expresión se llama descomposición de n factores primos. También es posible expresar el número 1 de esta forma tomando cada uno de los exponentes a_i iguales a 0.

Teorema 1.11. Si $n = \prod_{i=1}^r p_i^{a_i}$, el conjunto de los divisores positivos de n es el conjunto de los números de la forma $\prod_{i=1}^r p_i^{c_i}$, en donde $0 \leq c_i \leq a_i$ para $i = 1, 2, \dots, r$.

DEMOSTRACIÓN. Ejercicio.

Nota. Si escribimos los números primos en orden creciente, entonces:

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \dots, \quad p_n = \text{el } n\text{-ésimo primo},$$

cada entero positivo n (incluido el 1) se puede expresar en la forma

$$n = \prod_{i=1}^{\infty} p_i^{a_i}$$

en donde cada exponente $a_i \geq 0$. Los divisores positivos de n son todos los números de la forma

$$\prod_{i=1}^{\infty} p_i^{c_i}$$

en donde $0 \leq c_i \leq a_i$. Los productos son evidentemente finitos.

Teorema 1.12 Si dos enteros positivos a y b admiten las descomposiciones

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \quad b = \prod_{i=1}^{\infty} p_i^{b_i},$$

su mcd admite la descomposición

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

en donde cada $c_i = \min \{a_i, b_i\}$, el menor de a_i y b_i .

DEMOSTRACIÓN. Sea $d = \prod_{i=1}^{\infty} p_i^{c_i}$. Dado que $c_i \leq a_i$ y $c_i \leq b_i$ tenemos $d|a$ y $d|b$, luego d es un divisor común de a y b . Sea e otro divisor común de a y b , y con-

sideremos la descomposición de $e = \prod_{i=1}^{\infty} p_i^{e_i}$. Entonces $e_i \leq a_i$ y $e_i \leq b_i$ o sea $e_i \leq c_i$. Por lo tanto $e|d$, luego d es el mcd de a y b . $\square$

1.6 LA SERIE DE LOS INVERSOS DE LOS PRIMOS

Teorema 1.13 *La serie infinita $\sum_{n=1}^{\infty} 1/p_n$ diverge.*

DEMOSTRACIÓN. La siguiente demostración de este teorema se debe a Clarkson [11]. Suponemos que la serie converge y obtenemos una contradicción. Si la serie converge existe un entero k tal que

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}.$$

Sea $Q = p_1 \dots p_k$, y consideremos los números $1 + nQ$ para $n = 1, 2, \dots$. Ninguno de ellos es divisible por ninguno de los primos $p_1, \dots, p_k$. Por consiguiente, todos los factores primos de $1 + nQ$ se hallan entre los primos $p_{k+1}, p_{k+2}, \dots$. Por consiguiente, para cada $r \geq 1$ tenemos

$$\sum_{n=1}^r \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t,$$

puesto que la suma de la derecha contiene entre sus términos todos los términos de la izquierda. Pero el segundo miembro de esta desigualdad se halla dominado por la serie geométrica convergente

$$\sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t.$$

Por consiguiente la serie $\sum_{n=1}^{\infty} 1/(1+nQ)$ tiene sumas parciales acotadas y por lo tanto converge. Pero esto es contradictorio puesto que el criterio de la integral o el criterio de comparación del límite prueba que esta serie diverge. $\square$

Nota. La divergencia de la serie $\sum 1/p_n$ fue demostrada por primera vez en 1737 por Euler [20] que observó que implica el teorema de Euclides relativo a la existencia de una infinidad de primos.

En un capítulo posterior obtendremos una fórmula asintótica que demuestra que las sumas parciales $\sum_{k=1}^n 1/p_k$ tienden a infinito como $\log(\log n)$.

1.7 EL ALGORITMO DE EUCLIDES

El teorema 1.12 proporciona un método práctico para calcular el mcd (a, b) cuando se conocen las descomposiciones en factores primos de a y de b . Sin embargo, obtener estas descomposiciones en factores primos puede comportar considerables cálculos y es deseable disponer de un procedimiento que requiera menos esfuerzo. Existe un procedimiento útil conocido con el nombre de algoritmo de Euclides, que no requiere las descomposiciones de a y b . Este procedimiento se basa en divisiones sucesivas y hace uso del teorema que sigue.

Teorema 1.14. El algoritmo de división. *Dados dos enteros a y b con $b > 0$, existe un único par de enteros q y r tales que*

$$a = bq + r, \quad \text{con } 0 \leq r < b.$$

Además, $r = 0$ si, y sólo si, $b|a$.

Nota. Se dice que q es el *cociente* y r el *resto* obtenido al dividir a por b .

DEMOSTRACIÓN. Sea S el conjunto de enteros no negativos dado por

$$S = \{y : y = a - bx, \text{ } x \text{ es un entero, } y \geq 0\}.$$

Es un conjunto no vacío de enteros no negativos, por lo tanto admite mínimo, que designaremos $a - bq$. Sea $r = a - bq$. Entonces $a = bq + r$ y $r \geq 0$. Ahora demostraremos que $r < b$. Supongamos $r \geq b$. Entonces $0 \leq r - b < r$. Pero $r - b \in S$ ya que $r - b = a - b(q + 1)$. Por lo tanto $r - b$ es un elemento de S menor que su elemento mínimo r . Esta contradicción prueba que $r < b$. El par q, r es único, ya que si existiese otro par con estas condiciones q', r' , entonces $bq + r = bq' + r'$, de donde $b(q - q') = r' - r$. Luego $b|(r' - r)$. Si $r' - r \neq 0$ tendríamos $b \leq |r' - r|$, que constituye una contradicción. Por consiguiente $r' = r$ y $q' = q$. Finalmente es claro que $r = 0$ si, y sólo si, $b|a$.

Nota. A pesar de que el teorema 1.14 es un teorema de *existencia*, su demostración nos da un método para calcular el cociente q y el resto r . Restamos de a (o sumamos a a) múltiplos de b hasta obtener el menor número no negativo de la forma $a - bx$.

Teorema 1.15 El algoritmo de Euclides. Se dan dos enteros positivos a y b , tales que $b \nmid a$. Se escribe $r_0 = a$, $r_1 = b$, y aplicamos repetidamente el algoritmo de división obteniendo un conjunto de restos $r_2, r_3, \dots, r_n, r_{n+1}$ definidos sucesivamente por las relaciones

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{aligned}$$

Entonces r_n , el último resto no nulo de este proceso, es (a, b) , el mcd de a y b .

DEMOSTRACIÓN. Existe un momento en el que $r_{n+1} = 0$ puesto que los r_i son decrecientes y no negativos. La última relación, $r_{n-1} = r_n q_n$ demuestra que $r_n | r_{n-1}$. La anterior a la última prueba que $r_n | r_{n-2}$. Por inducción vemos que r_n divide a cada r_i . En particular $r_n | r_1 = b$ y $r_n | r_0 = a$, luego r_n es un divisor común de a y b . Ahora sea d otro divisor común de a y b . La definición de r_2 prueba que $d | r_2$. La relación que le sigue prueba que $d | r_3$. Por inducción, d divide a cada r_i luego $d | r_n$. Por lo tanto r_n es el mcd requerido. $\square$

1.8 EL MÁXIMO COMÚN DIVISOR DE MÁS DE DOS NÚMEROS

El máximo común divisor de tres enteros a, b, c se designa (a, b, c) y se define por la relación

$$(a, b, c) = (a, (b, c)).$$

Por el teorema 1.4(b) tenemos $(a, (b, c)) = ((a, b), c)$ luego el mcd depende únicamente de a, b, c y no del orden en el que estén escritos.

Análogamente, el mcd de n enteros $a_1, \dots, a_n$ se define inductivamente por la relación

$$(a_1, \dots, a_n) = (a_1, (a_2, \dots, a_n)).$$

De nuevo, este número es independiente del orden en que aparecen los a_i .

Si $d = (a_1, \dots, a_n)$ es fácil comprobar que d divide a cada uno de los a_i y que cada divisor común divide a d . Además, d es combinación lineal de los a_i . Es decir, existen enteros $x_1, \dots, x_n$ tales que

$$(a_1, \dots, a_n) = a_1x_1 + \dots + a_nx_n.$$

Si $d = 1$ los números se llaman *primos entre sí*. Por ejemplo 2, 3 y 10 son primos entre sí.

Si $(a_i, a_j) = 1$ siempre que $i \neq j$ se dice que los números $a_1, \dots, a_n$ son *primos entre sí dos a dos*. Si $a_1, \dots, a_n$ son primos entre sí dos a dos, entonces $(a_1, \dots, a_n) = 1$. Sin embargo, el ejemplo (2, 3, 10) muestra que el recíproco no es necesariamente verdadero.

Ejercicios del capítulo 1

En estos ejercicios las letras latinas minúsculas $a, b, c, \dots, x, y, z$ representan enteros.

Probar cada una de las afirmaciones de los ejercicios 1 al 6.

1. Si $(a, b) = 1$ y si $c|a$ y $d|b$, entonces $(c, d) = 1$.
2. Si $(a, b) = (a, c) = 1$, entonces $(a, bc) = 1$.
3. Si $(a, b) = 1$, entonces $(a^n, b^k) = 1$ para todo $n \geq 1, k \geq 1$.
4. Si $(a, b) = 1$, entonces $(a + b, a - b)$ o es 1 o es 2.
5. Si $(a, b) = 1$, entonces $(a + b, a^2 - ab + b^2)$ o es 1 o es 3.
6. Si $(a, b) = 1$ y si $d|(a + b)$, entonces $(a, d) = (b, d) = 1$.
7. Un número racional a/b con $(a, b) = 1$ se llama *fracción reducida*. Si la suma de dos fracciones reducidas es un entero, es decir, si $(a/b) + (c/d) = n$. Demostrar que entonces $|b| = |d|$.
8. Un entero se llama *sin cuadrados* si no es divisible por el cuadrado de ningún primo. Probar que, para cada $n \geq 1$, existen $a > 0$ y $b > 0$, unívocamente determinados, tales que $n = a^2b$, en donde b es sin cuadrados.
9. Para cada una de las afirmaciones que siguen, dar una demostración o un contraejemplo.
 - (a) Si $b^2|n$ y $a^2|n$ y $a^2 \leq b^2$, entonces $a|b$.
 - (b) Si b^2 es el mayor cuadrado que divide a n , entonces $a^2|n$ implica $a|b$.
10. Dados x e y , sean $m = ax + by, n = cx + dy$, en donde $ad - bc = \pm 1$. Probar que $(m, n) = (x, y)$.
11. Probar que, si $n > 1, n^4 + 4$ es compuesto.

En los ejercicios 12, 13 y 14, a, b, c, m y n designan enteros *positivos*.

12. Establecer una demostración o un contraejemplo para cada una de las afirmaciones siguientes.
 - (a) Si $a^n|b^n$, entonces $a|b$.
 - (b) Si $n^n|m^m$, entonces $n|m$.
 - (c) Si $a^n|2b^n$ y $n > 1$, entonces $a|b$.
13. Si $(a, b) = 1$ y $(a/b)^m = n$, probar que $b = 1$.
 - (b) Si n no es la potencia m -ésima de un entero positivo, entonces $n^{1/m}$ es irracional.
14. Si $(a, b) = 1$ y $ab = c^n$, probar que $a = x^n$ y $b = y^n$ para algún x y algún y . [Indicación: Considerar $d = (a, c)$.]

15. Probar que cada $n \geq 12$ es la suma de dos números compuestos.
16. Probar que, si $2^n - 1$ es primo, entonces n es primo.
17. Probar que, si $2^n + 1$ es primo, entonces n es una potencia de 2.
18. Si $m \neq n$ calcular el mcd $(a^{2m} + 1, a^{2n} + 1)$ en términos de a . [Indicación: Sea $A_n = a^{2n} + 1$ y probar que $A_n | (A_m - 2)$ si $m > n$.]
19. La sucesión de Fibonacci 1, 1, 2, 3, 5, 8, 13, 21, 34, ... se define por medio de la fórmula de recursión $a_{n+1} = a_n + a_{n-1}$, con $a_1 = a_2 = 1$. Probar que, para cada n , $(a^n, a_{n+1}) = 1$.
20. Sea $d = (826, 1890)$. Utilizar el algoritmo de Euclides para calcular d , y expresar entonces d como combinación lineal de 826 y 1890.
21. El mínimo común múltiplo (mcm) de dos enteros a y b se designa por $[a, b]$ o por aMb , y se define como sigue:

$$[a, b] = |ab|/(a, b) \quad \text{si } a \neq 0 \text{ y } b \neq 0,$$

$$[a, b] = 0 \quad \text{si } a = 0 \text{ o } b = 0.$$

Probar que el mcm posee las siguientes propiedades:

- (a) si $a = \prod_{i=1}^{\infty} p_i^{a_i}$ y $b = \prod_{i=1}^{\infty} p_i^{b_i}$ entonces $[a, b] = \prod_{i=1}^{\infty} p_i^{c_i}$, donde $c_i = \max\{a_i, b_i\}$.
- (b) $(aDb)Mc = (aMc)D(bMc)$.
- (c) $(aMb)Dc = (aDc)M(bDc)$.

(D y M son distributivas una con respecto de la otra.)

22. Probar que $(a, b) = (a + b, [a, b])$.
23. La suma de dos enteros positivos es 5264 y su mínimo común múltiplo es 200340. Determinar ambos enteros.
24. Probar la siguiente propiedad multiplicativa del mcd:

$$(ah, bk) = (a, b)(h, k) \left(\frac{a}{(a, b)}, \frac{k}{(h, k)} \right) \left(\frac{b}{(a, b)}, \frac{h}{(h, k)} \right).$$

En particular, si $(a, b) = (h, k) = 1$, dicha propiedad prueba que $(ah, bk) = (a, k)(b, h)$.

Probar cada una de las afirmaciones de los ejercicios 25 al 28. Todos los enteros son positivos.

25. Si $(a, b) = 1$ existe un $x > 0$ y un $y > 0$ tales que $ax - by = 1$.
26. Si $(a, b) = 1$ y $x^a = y^b$ entonces $x = n^b$ e $y = n^a$ para un cierto n . [Indicación: Usar los ejercicios 25 y 13.]
27. (a) Si $(a, b) = 1$ entonces, para cada $n > ab$, existen positivos x e y tales que $n = ax + by$.
(b) Si $(a, b) = 1$ no existen positivos x e y tales que $ab = ax + by$.
28. Si $a > 1$, entonces $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$.
29. Dado $n > 0$, sea S un conjunto cuyos elementos sean enteros positivos $\leq 2n$ tales que, si a y b pertenecen a S y $a \neq b$, entonces $a \nmid b$. ¿Cuál es el máximo número de enteros que puede contener S ? [Indicación: S puede contener, a lo sumo, uno de los enteros 1, 2, 2^2 , 2^3 , ..., a lo sumo uno de los enteros 3, $3 \cdot 2$, $3 \cdot 2^2$, ..., etc.]

30. Si $n > 1$ probar que la suma

$$\sum_{k=1}^n \frac{1}{k}$$

no es un entero.

Capítulo 2

Funciones aritméticas y producto de Dirichlet

2.1 INTRODUCCIÓN

La Teoría de números, como muchas otras partes de las Matemáticas, trata a menudo con sucesiones de números reales o complejos. En Teoría de números tales sucesiones se llaman *funciones aritméticas*.

Definición. Una función real —o compleja— definida sobre los enteros positivos se llama una función aritmética o una función de Teoría de números.

Este capítulo introduce varias funciones aritméticas que juegan un papel importante en el estudio de las propiedades de la divisibilidad de enteros y en la distribución de primos. El capítulo discute también la multiplicación de Dirichlet, un concepto que sirve para clarificar interrelaciones entre varias funciones aritméticas.

Empezaremos con dos ejemplos importantes, la *función de Möbius* $\mu(n)$ y la *función indicatriz de Euler* $\varphi(n)$.

2.2 LA FUNCIÓN DE MÖBIUS $\mu(n)$

Definición. La función de Möbius μ se define como sigue:

$$\mu(1) = 1;$$

Si $n > 1$, escribimos $n = p_1^{a_1} \dots p_k^{a_k}$. Entonces

$$\begin{aligned}\mu(n) &= (-1)^k \text{ si } a_1 = a_2 = \dots = a_k = 1, \\ \mu(n) &= 0 \text{ en otro caso.}\end{aligned}$$

Obsérvese que $\mu(n) = 0$ si, y sólo si, n admite un divisor cuadrado > 1 .

He aquí una breve tabla de valores de $\mu(n)$:

n :	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

La función de Möbius interviene en diferentes lugares en Teoría de números. Una de sus principales propiedades es una fórmula simple, pero notable, relativa a la suma $\sum_{d|n} \mu(d)$, extendida sobre los divisores positivos de n . En esta fórmula $[x]$ designa el mayor entero $\leq x$.

Teorema 2.1 Si $n \geq 1$ tenemos

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n} \right] = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

DEMOSTRACIÓN. La fórmula es claramente cierta para $n = 1$. Suponemos, entonces, que $n > 1$ y escribimos $n = p_1^{a_1} \dots p_k^{a_k}$. En la suma $\sum_{d|n} \mu(d)$ los únicos términos no nulos proceden de $d = 1$ y de los divisores de n que son productos de primos distintos. Entonces

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \dots + \mu(p_k) + \mu(p_1 p_2) + \dots + \mu(p_{k-1} p_k) \\ &\quad + \dots + \mu(p_1 p_2 \dots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k = (1 - 1)^k = 0. \quad \square\end{aligned}$$

2.3 LA FUNCIÓN INDICATRIZ DE EULER $\varphi(n)$

Definición. Si $n \geq 1$ la indicatriz de Euler $\varphi(n)$ es el número de enteros positivos menores que n que son primos con n ; así pues,

$$(1) \quad \varphi(n) = \sum_{k=1}^n{}' 1,$$

en donde la ' indica que la suma se halla extendida sobre los k primos con n .

He aquí una breve tabla de valores de $\mu(n)$:

n :	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Como en el caso de $\mu(n)$ existe una fórmula simple para la suma $\sum_{d|n} \varphi(d)$.

Teorema 2.2 Si $n \geq 1$ tenemos

$$\sum_{d|n} \varphi(d) = n.$$

DEMOSTRACIÓN. Si S designa el conjunto $\{1, 2, \dots, n\}$, distribuimos los enteros de S en conjuntos disjuntos de la forma siguiente. Para cada divisor d de n , sea

$$A(d) = \{k: (k, n) = d, 1 \leq k \leq n\}.$$

Esto es, $A(d)$ contiene los elementos de S cuyo mcd con n es d . Los conjuntos $A(d)$ constituyen una partición de S . Por consiguiente, si $f(d)$ designa el número de enteros de $A(d)$, tenemos

$$(2) \quad \sum_{d|n} f(d) = n.$$

Pero $(k, n) = d$ si, y sólo si, $(k/d, n/d) = 1$, y $0 < k \leq n$ si, y sólo si, $0 < k/d \leq n/d$. Por consiguiente, si hacemos $q = k/d$, existe una correspondencia uno a uno entre los elementos de $A(d)$ y los enteros q que satisfacen $0 < q \leq n/d$, $(q, n/d) = 1$. El número de tales q es $\varphi(n/d)$. Por lo tanto $f(d) = \varphi(n/d)$ y (2) nos conduce a

$$\sum_{d|n} \varphi(n/d) = n.$$

Pero esto es equivalente a la igualdad $\sum_{d|n} \varphi(d) = n$ puesto que d recorre todos los divisores de n o sea los n/d . Y esto completa la demostración. $\square$

2.4 UNA RELACIÓN QUE CONECTA φ Y μ

La indicatriz de Euler está relacionada con la función de Möbius por medio de la fórmula que sigue:

Teorema 2.3 Si $n \geq 1$ tenemos

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

DEMOSTRACIÓN. La suma (1) que define $\varphi(n)$ se puede escribir en la forma

$$\varphi(n) = \sum_{k=1}^n \left[\frac{1}{(n, k)} \right],$$

en donde k recorre todos los enteros $\leq n$. Ahora utilizamos el teorema 2.1 substituyendo n por (n, k) y obtenemos

$$\varphi(n) = \sum_{k=1}^n \sum_{d|(n, k)} \mu(d) = \sum_{k=1}^n \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Para un divisor d de n fijo podemos sumar respecto de todos los k tales que $1 \leq k \leq n$ que son múltiplos de d . Si escribimos $k = qd$ entonces $1 \leq k \leq n$ si, y sólo si, $1 \leq q \leq n/d$. Por lo tanto la última suma que da $\varphi(n)$ se puede escribir

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Esto demuestra el teorema. $\square$

2.5 UNA FÓRMULA PRODUCTO PARA $\varphi(n)$

La suma que define $\varphi(n)$ en el teorema 2.3 se puede expresar también como un producto extendido a los divisores primos de n , distintos.

Teorema 2.4 Para $n \geq 1$ tenemos

$$(3) \quad \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

DEMOSTRACIÓN. Para $n = 1$ el producto es vacío puesto que no existe ningún primo que divida a 1. En este caso entendemos que al producto se le asigna el valor 1

Suponemos, entonces, que $n > 1$ y que $p_1, \dots, p_r$ son los divisores primos distintos de n . El producto se puede escribir

$$(4) \quad \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \\ = 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \dots + \frac{(-1)^r}{p_1 p_2 \dots p_r}.$$

En el segundo miembro entendemos que en un término como $\sum 1/p_i p_j p_k$ se consideran todos los posibles productos $p_i p_j p_k$ de factores primos distintos de n , tomando tres de ellos a un tiempo. Obsérvese que cada uno de los términos de la derecha de (4) es de la forma $\pm 1/d$, en donde d es un divisor de n que es 1 o un producto de primos distintos. El numerador ± 1 es exactamente $\mu(d)$. Puesto que $\mu(d) = 0$ si d es divisible por el cuadrado de algún p_i vemos que la suma de (4) es exactamente la misma que

$$\sum_{d|n} \frac{\mu(d)}{d}.$$

Esto prueba el teorema. □

Muchas de las propiedades de $\varphi(n)$ se pueden deducir fácilmente de esta fórmula del producto. Se dan algunas de ellas en el siguiente teorema

Teorema 2.5 La indicatriz de Euler posee las siguientes propiedades:

- (a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ para p primo y $\alpha \geq 1$.
- (b) $\varphi(mn) = \varphi(m)\varphi(n)$ ($d|\varphi(d)$), en donde $d = (m, n)$.
- (c) $\varphi(mn) = \varphi(m)\varphi(n)$ si $(m, n) = 1$.
- (d) $a|b$ implica $\varphi(a)|\varphi(b)$.

(e) $\varphi(n)$ es par para $n \geq 3$. Además, si n posee r factores primos impares distintos, entonces $2^r | \varphi(n)$.

DEMOSTRACIÓN. La parte (a) se obtiene inmediatamente si en (3) hacemos $n = p^a$. Para probar (b) escribimos

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Ahora observamos que cada divisor primo de mn es un divisor primo de m o de n , y aquellos divisores primos que dividen tanto a m como a n dividen también a (m, n) . Por lo tanto

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)} \left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m} \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}},$$

por lo que obtenemos (b). La parte (c) es un caso especial de la parte (b).

Ahora deducimos (d) de (b). Dado que $a|b$ tenemos $b = ac$ en donde $1 \leq c \leq b$. Si $c = b$, entonces $a = 1$ y la parte (d) se verifica trivialmente. Por consiguiente, suponemos que $c < b$. De (b) tenemos

$$(5) \quad \varphi(b) = \varphi(ac) = \varphi(a)\varphi(c) \frac{d}{\varphi(d)} = d\varphi(a) \frac{\varphi(c)}{\varphi(d)},$$

en donde $d = (a, c)$. Ahora el resultado se obtiene por inducción sobre b . Para $b = 1$ se sigue trivialmente. Suponemos, pues, que (d) se verifica para todo entero $< b$. Entonces se verifica para c luego, puesto que $d|c$, $\varphi(d)|\varphi(c)$. Por lo que el segundo miembro de (5) es un múltiplo de $\varphi(a)$, es decir, $\varphi(a)|\varphi(b)$. Esto prueba (d).

Ahora demostraremos (e). Si $n = 2^\alpha$, $\alpha \geq 2$, la parte (a) prueba que $\varphi(n)$ es par. Si n posee, por lo menos, un divisor primo escribimos

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1) = c(n) \prod_{p|n} (p-1),$$

en donde $c(n)$ es un entero. El producto que multiplica a $c(n)$ es par así que $\varphi(n)$ es par. Además, cada primo impar p proporciona un factor 2 a este producto, por lo tanto $2^r | \varphi(n)$ si n tiene r factores primos impares distintos. $\square$

2.6 EL PRODUCTO DE DIRICHLET DE FUNCIONES ARITMÉTICAS

En el teorema 2.3 hemos probado que

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

La suma del segundo miembro es de un tipo que interviene frecuentemente en Teoría de números. Estas sumas tienen la forma

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

en donde f y g son funciones aritméticas, y merece la pena estudiar algunas propiedades que estas sumas tienen en común. Veremos más adelante que las sumas de este tipo aparecen de forma natural en la teoría de las series de Dirichlet. Resulta de utilidad tratar estas sumas como un nuevo tipo de multiplicación de funciones aritméticas, punto de vista introducido por E. T. Bell [4] en 1915.

Definición. Si f y g son dos funciones aritméticas definimos su producto de Dirichlet (o convolución de Dirichlet) como la función aritmética h definida por

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Notación. Escribiremos $f * g$ en vez de h y $(f * g)(n)$ en vez de $h(n)$. El símbolo N se utilizará para la función aritmética tal que $N(n) = n$ para todo n . Con esta notación, el teorema 2.3 se puede establecer en la forma

$$\varphi = \mu * N.$$

El teorema que sigue describe propiedades algebraicas de la multiplicación de Dirichlet.

Teorema 2.6. *La multiplicación de Dirichlet es asociativa y conmutativa. Esto es, para toda terna de funciones aritméticas f, g, k , tenemos*

$$\begin{aligned} f * g &= g * f && (\text{ley conmutativa}) \\ (f * g) * k &= f * (g * k) && (\text{ley asociativa}). \end{aligned}$$

DEMOSTRACIÓN. Observemos ante todo que la definición de $f * g$ se puede expresar como sigue

$$(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b),$$

en donde a y b varían sobre el conjunto de todos los enteros positivos cuyo producto es n . Esto hace evidente la propiedad conmutativa.

Para probar la propiedad asociativa sea $A = g * k$ y consideremos $f * A = f * (g * k)$. Tenemos

$$\begin{aligned} (f * A)(n) &= \sum_{a \cdot d = n} f(a)A(d) = \sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b)k(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a)g(b)k(c). \end{aligned}$$

De la misma forma, si $B = f * g$ y consideramos $B * k$ obtenemos la misma fórmula para $(B * k)(n)$. Por lo tanto $f * A = B * k$ lo que indica que la multiplicación de Dirichlet es asociativa. $\square$

Ahora introducimos un elemento identidad para esta multiplicación.

Definición. La función aritmética I dada por.

$$I(n) = \begin{bmatrix} 1 \\ n \end{bmatrix} = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

se llama la función identidad.

Teorema 2.7 *Para todo f se tiene $I * f = f * I = f$.*

DEMOSTRACIÓN. Tenemos

$$(f * I)(n) = \sum_{d|n} f(d)I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\left[\frac{d}{n}\right] = f(n)$$

ya que $[d/n] = 0$ si $d < n$.

2.7 INVERSOS DE DIRICHLET Y FÓRMULA DE INVERSIÓN DE MÖBIUS

Teorema 2.8 Si f es una función aritmética con $f(1) \neq 0$ existe una única función aritmética f^{-1} , llamada inversa de Dirichlet de f , tal que

$$f * f^{-1} = f^{-1} * f = I.$$

Además, f^{-1} se obtiene por medio de las fórmulas de recurrencia

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \text{para } n > 1.$$

DEMOSTRACIÓN. Dada f , veremos que la ecuación $(f * f^{-1})(n) = I(n)$ tiene una solución única dada por los valores de la función $f^{-1}(n)$. Para $n = 1$ debemos resolver la ecuación

$$(f * f^{-1})(1) = I(1)$$

que se reduce a

$$f(1)f^{-1}(1) = 1.$$

Puesto que $f(1) \neq 0$ existe una solución y sólo una, que es $f^{-1}(1) = 1/f(1)$. Ahora suponemos que los valores funcionales $f^{-1}(k)$ se han determinado de forma única para todo $k < n$. Entonces debemos resolver la ecuación $(f * f^{-1})(n) = I(n)$, o bien

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Podemos escribirla en la forma

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right)f^{-1}(d) = 0.$$

Si conocemos los valores $f^{-1}(d)$ para todo divisor $d < n$, existe un valor unívocamente determinado para $f^{-1}(n)$, a saber,

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right)f^{-1}(d),$$

puesto que $f(1) \neq 0$. Esto establece la existencia y unicidad de f^{-1} por inducción. $\square$

Nota. Tenemos $(f * g)(1) = f(1)g(1)$. Luego, si $f(1) \neq 0$ y $g(1) \neq 0$, entonces $(f * g)(1) \neq 0$. Este hecho, junto con los teoremas 2.6, 2.7 y 2.8, nos dice que, en el lenguaje de la teoría de grupos, el conjunto de todas las funciones aritméticas f con $f(1) \neq 0$ constituye un grupo abeliano con respecto de la operación $*$, siendo el elemento neutro la función I . El lector puede verificar con facilidad que

$$(f * g)^{-1} = f^{-1} * g^{-1} \quad \text{si } f(1) \neq 0 \text{ y } g(1) \neq 0.$$

Definición. Definimos la función unidad u como la función aritmética tal que $u(n) = 1$ para todo n .

El teorema 2.1 establece que $\sum_{d|n} \mu(d) = I(n)$. Con la notación de la multiplicación de Dirichlet se expresa

$$\mu * u = I.$$

Entonces u y μ son inversas de Dirichlet una de otra:

$$u = \mu^{-1} \quad \text{y} \quad \mu = u^{-1}.$$

Esta propiedad simple de la función de Möbius, junto con la asociatividad de la multiplicación de Dirichlet, nos permite establecer una demostración simple del teorema que sigue.

Teorema 2.9 Fórmula de inversión de Möbius. *La ecuación*

$$(6) \quad f(n) = \sum_{d|n} g(d)$$

implica

$$(7) \quad g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right).$$

Recíprocamente, (7) implica (6).

DEMOSTRACIÓN. La ecuación (6) establece que $f = g * u$. Multiplicando por μ obtenemos $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$, que es (7). Recíprocamente, la multiplicación de $f * \mu = g$ por u nos da (6). $\square$

La fórmula de inversión de Möbius ha sido ilustrada ya por el par de fórmulas de los teoremas 2.2 y 2.3:

$$n = \sum_{d|n} \varphi(d), \quad \varphi(n) = \sum_{d|n} d \mu\left(\frac{n}{d}\right).$$

2.8 LA FUNCIÓN DE MANGOLDT $\Lambda(n)$

Ahora introducimos la función de Mangoldt Λ que juega un papel central en la distribución de primos.

Definición. Para cada entero $n \geq 1$ definimos

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ para un cierto primo } p \text{ y un cierto } m \geq 1, \\ 0 & \text{en otro caso.} \end{cases}$$

He aquí una tabla breve de valores de $\Lambda(n)$:

n :	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

La demostración del teorema que sigue muestra cómo esta función surge naturalmente del teorema fundamental de la Aritmética.

Teorema 2.10 Si $n \geq 1$ tenemos

$$(8) \quad \log n = \sum_{d|n} \Lambda(d).$$

DEMOSTRACIÓN. El teorema es cierto para $n = 1$ ya que ambos miembros son 0. Por consiguiente, suponemos que $n > 1$ y escribimos

$$n = \prod_{k=1}^r p_k^{a_k}.$$

Tomando logaritmos tenemos

$$\log n = \sum_{k=1}^r a_k \log p_k.$$

Ahora consideramos la suma del segundo miembro de (8). Los únicos términos no nulos de la suma provienen de los divisores d de la forma p_k^m para $m = 1, 2, \dots, a_k$ y $k = 1, 2, \dots, r$. Luego

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^r \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^r \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^r a_k \log p_k = \log n,$$

que prueba (8). □

Ahora utilizamos la inversión de Möbius para expresar $\Lambda(n)$ en términos del logaritmo.

Teorema 2.11 Si $n \geq 1$ tenemos

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = - \sum_{d|n} \mu(d) \log d.$$

DEMOSTRACIÓN. Invirtiendo (8) por la fórmula de inversión de Möbius obtenemos

$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= I(n) \log n - \sum_{d|n} \mu(d) \log d. \end{aligned}$$

Puesto que $I(n) \log n = 0$ para todo n , la demostración queda establecida. $\square$

2.9 FUNCIONES MULTIPLICATIVAS

Hemos observado ya que el conjunto de todas las funciones aritméticas f con $f(1) \neq 0$ forma un grupo abeliano respecto de la multiplicación de Dirichlet. En esta sección discutimos un subgrupo de este importante grupo, llamado de las funciones *multiplicativas*.

Definición. Una función aritmética f se llama función multiplicativa si f no es idénticamente nula y si

$$f(mn) = f(m)f(n) \quad \text{siempre que } (m, n) = 1.$$

Una función multiplicativa f se llama completamente multiplicativa si verifica

$$f(mn) = f(m)f(n) \quad \text{para todo } m, n.$$

EJEMPLO 1 Sea $f_\alpha(n) = n^\alpha$, en donde α es un número real o complejo fijo. Esta función es completamente multiplicativa. En particular, la función unidad $u = f_0$ es completamente multiplicativa. La función f_α la designaremos por N^α y la llamaremos función potencia.

EJEMPLO 2 La función identidad $I(n) = [1/n]$ es completamente multiplicativa.

EJEMPLO 3 La función de Möbius es multiplicativa pero no es completamente multiplicativa. Es fácil verlo a partir de la definición de $\mu(n)$. Consideremos dos primos relativos m y n . Si m o n posee un divisor que es cuadrado de un primo también lo posee mn , y tanto $\mu(mn)$ como $\mu(m)\mu(n)$ son cero. Si ninguno de ellos contiene un divisor cuadrático, entonces $m = p_1 \dots p_s$ y $n = q_1 \dots q_t$ en donde los p_i y los q_i son primos distintos. Luego $\mu(m) = (-1)^s$, $\mu(n) = (-1)^t$ y $\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$. Ello demuestra que μ es multiplicativa. No es completamente multiplicativa puesto que $\mu(4) = 0$ y, en cambio, $\mu(2)\mu(2) = 1$.

EJEMPLO 4 La indicatriz de Euler $\varphi(n)$ es multiplicativa. Esta es la parte (c) del teorema 2.5. No es completamente multiplicativa puesto que $\varphi(4) = 2$ mientras que $\varphi(2)\varphi(2) = 1$.

EJEMPLO 5 El producto ordinario fg de dos funciones aritméticas f y g se define por medio de la fórmula usual

$$(fg)(n) = f(n)g(n).$$

Análogamente, el cociente f/g se define por medio de la fórmula

$$\left(\frac{f}{g}\right)(n) = \frac{f(n)}{g(n)} \quad \text{siempre que } g(n) \neq 0.$$

Si f y g son multiplicativas, fg y f/g también lo son. Si f y g son completamente multiplicativas, también lo son fg y f/g .

Deducimos ahora algunas propiedades comunes a todas las funciones multiplicativas.

Teorema 2.12 Si f es multiplicativa, entonces $f(1) = 1$.

DEMOSTRACIÓN. Tenemos $f(n) = f(1)f(n)$ puesto que $(n, 1) = 1$ para todo n . Dado que f no es idénticamente nula tenemos $f(n) \neq 0$ para algún n , luego $f(1) = 1$. $\square$

Nota. Puesto que $\Lambda(1) = 0$, la función de Mangoldt no es multiplicativa.

Teorema 2.13 Dada f con $f(1) = 1$, entonces:

(a) f es multiplicativa si, y sólo si,

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$$

para todos los primos p_i y todos los enteros $a_i \geq 1$.

(b) Si f es multiplicativa, entonces f es completamente multiplicativa si, y sólo si,

$$f(p^a) = f(p)^a$$

para todos los primos p y todos los enteros $a \geq 1$.

DEMOSTRACIÓN. La demostración se deduce fácilmente de las definiciones y se deja como ejercicio al lector.

2.10 FUNCIONES MULTIPLICATIVAS Y PRODUCTO DE DIRICHLET

Teorema 2.14 Si f y g son multiplicativas, también lo es su producto de Dirichlet $f * g$.

DEMOSTRACIÓN. Sea $h = f * g$ y elijamos dos enteros primos entre sí m y n . Entonces

$$h(mn) = \sum_{c|mn} f(c)g\left(\frac{mn}{c}\right).$$

Ahora bien cada divisor c de mn se puede expresar en la forma $c = ab$ en donde $a|m$ y $b|n$. Además, $(a, b) = 1$, $(m/a, n/b) = 1$, y existe una correspondencia uno a uno entre el conjunto de los productos ab y el de los divisores c de mn . Por lo tanto

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) = h(m)h(n). \end{aligned}$$

Esto termina la demostración. □

Advertencia. El producto de Dirichlet de dos funciones completamente multiplicativas no es necesariamente completamente multiplicativo.

Una ligera modificación en la demostración precedente nos permite probar:

Teorema 2.15 Si g y $f * g$ son multiplicativas, f también es multiplicativa.

DEMOSTRACIÓN. Supondremos que f no es multiplicativa y deduciremos que $f * g$ tampoco lo es. Sea $h = f * g$. Dado que f no es multiplicativa existen enteros positivos m y n con $(m, n) = 1$ tales que

$$f(mn) \neq f(m)f(n).$$

Elegimos el par m, n de forma que el producto mn sea mínimo.

Si $mn = 1$ entonces $f(1) \neq f(1)f(1)$ luego $f(1) \neq 1$. Por lo tanto $h(1) = f(1)g(1) = f(1) \neq 1$, que demuestra que h no es multiplicativa.

Si $mn > 1$, entonces tenemos $f(ab) = f(a)f(b)$ para todo par de enteros positivos a y b con $(a, b) = 1$ y $ab < mn$. Ahora argüimos como en la demostración del teorema 2.14, con la excepción de que en la suma que define $h(mn)$ separamos los términos que corresponden a $a = m$, $b = n$. Entonces tenemos

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n \\ ab < mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) = \sum_{\substack{a|m \\ b|n \\ ab < mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn) \\ &= h(m)h(n) - f(m)f(n) + f(mn). \end{aligned}$$

Puesto que $f(mn) \neq f(m)f(n)$ esto demuestra que $h(mn) \neq h(m)h(n)$, luego h no es multiplicativa. Esta contradicción termina la demostración. $\square$

Teorema 2.16 Si g es multiplicativa, también lo es su inversa de Dirichlet g^{-1} .

DEMOSTRACIÓN. Se deduce inmediatamente del teorema 2.15 ya que g y $g * g^{-1} = I$ son ambas multiplicativas. (Ver ejercicio 2.34 para otra demostración.) $\square$

Nota. Los teoremas 2.14 y 2.16 demuestran que el conjunto de las funciones multiplicativas constituye un subgrupo del grupo de todas las funciones aritméticas f con $f(1) \neq 0$.

2.11 LA INVERSA DE UNA FUNCIÓN COMPLETAMENTE MULTIPLICATIVA

La inversa de Dirichlet de una función completamente multiplicativa es particularmente fácil de calcular.

Teorema 2.17 Sea f multiplicativa. Entonces f es completamente multiplicativa si, y sólo si,

$$f^{-1}(n) = \mu(n)f(n) \quad \text{para todo } n \geq 1.$$

DEMOSTRACIÓN. Sea $g(n) = \mu(n)f(n)$. Si f es completamente multiplicativa tenemos

$$(g * f)(n) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n) I(n) = I(n)$$

puesto que $f(1) = 1$ e $I(n) = 0$ para $n > 1$. Luego $g = f^{-1}$.

Recíprocamente, suponemos $f^{-1}(n) = \mu(n)f(n)$. Para probar que f es completamente multiplicativa basta demostrar que $f(p^a) = f(p)^a$ para potencias de primos. La ecuación $f^{-1}(n) = \mu(n)f(n)$ implica que

$$\sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = 0 \quad \text{para todo } n > 1.$$

Luego, si tomamos $n = p^a$, tenemos

$$\mu(1)f(1)f(p)^a + \mu(p)f(p)f(p^{a-1}) = 0,$$

de lo que obtenemos $f(p^a) = f(p)f(p^{a-1})$. Ello implica $f(p^a) = f(p)^a$, luego f es completamente multiplicativa. $\square$

EJEMPLO La inversa de la función φ de Euler. Puesto que $\varphi = \mu * N$ tenemos $\varphi^{-1} = \mu^{-1} * N^{-1}$. Pero $N^{-1} = \mu N$ puesto que N es completamente multiplicativa, luego

$$\varphi^{-1} = \mu^{-1} * \mu N = \mu * \mu N.$$

Por lo tanto

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d).$$

El teorema que sigue demuestra que

$$\varphi^{-1}(n) = \prod_{p|n} (1 - p).$$

Teorema 2.18 Si f es multiplicativa tenemos

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p)).$$

DEMOSTRACIÓN. Sea

$$g(n) = \sum_{d|n} \mu(d)f(d).$$

Entonces g es multiplicativa, luego para determinar $g(n)$ es suficiente calcular $g(p^a)$. Pero

$$g(p^a) = \sum_{d|p^a} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p).$$

Luego

$$g(n) = \prod_{p|n} g(p^a) = \prod_{p|n} (1 - f(p)). \quad \square$$

2.12 LA FUNCIÓN $\lambda(n)$ DE LIOUVILLE

Un ejemplo importante de función completamente multiplicativa es la función λ de Liouville, que se define como sigue.

Definición. Definimos $\lambda(1) = 1$, y si $n = p_1^{a_1} \dots p_k^{a_k}$ definimos

$$\lambda(n) = (-1)^{a_1 + \dots + a_k}.$$

La definición muestra que λ es completamente multiplicativa. El teorema que sigue describe la suma de λ extendida a los divisores de n .

Teorema 2.19 Para cada $n \geq 1$ tenemos

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n \text{ es un cuadrado} \\ 0 & \text{en otro caso.} \end{cases}$$

Además, $\lambda^{-1}(n) = |\mu(n)|$ para todo n .

DEMOSTRACIÓN. Sea $g(n) = \sum_{d|n} \lambda(d)$. Entonces g es multiplicativa, luego para determinar $g(n)$ únicamente necesitamos calcular $g(p^a)$ para potencias de primos. Tenemos

$$g(p^a) = \sum_{d|p^a} \lambda(d) = 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a)$$

$$= 1 - 1 + 1 - \cdots + (-1)^a = \begin{cases} 0 & \text{si } a \text{ es impar,} \\ 1 & \text{si } a \text{ es par.} \end{cases}$$

Por lo tanto, si $n = \prod_{i=1}^k p_i^{a_i}$, tenemos $g(n) = \prod_{i=1}^k g(p_i^{a_i})$. Si un exponente a_i es impar, entonces $g(p_i^{a_i}) = 0$, luego $g(n) = 0$. Si todos los exponentes a_i son pares, entonces $g(p_i^{a_i}) = 1$ para todo i y $g(n) = 1$. Esto prueba que $g(n) = 1$ si n es un cuadrado, y $g(n) = 0$ en otro caso. Por consiguiente, $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$.

2.13 LAS FUNCIONES DIVISOR $\sigma_\alpha(n)$

Definición. Para todo real o complejo α y todo entero $n \geq 1$ definimos

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

suma de las potencias α -ésimas de los divisores de n .

Las funciones σ_α así definidas se llaman *funciones divisores*. Son multiplicativas puesto que $\sigma_\alpha = u * N^\alpha$, producto de Dirichlet de dos funciones multiplicativas.

Cuando $\alpha = 0$, $\sigma_0(n)$ es el *número* de divisores de n ; a menudo se designa $d(n)$.

Cuando $\alpha = 1$, $\sigma_1(n)$ es la *suma* de los divisores de n ; a menudo se designa $\sigma(n)$.

Dado que σ_α es multiplicativa tenemos

$$\sigma_\alpha(p_1^{a_1} \cdots p_k^{a_k}) = \sigma_\alpha(p_1^{a_1}) \cdots \sigma_\alpha(p_k^{a_k}).$$

Para calcular $\sigma_\alpha(p^a)$ observamos que los divisores de una potencia de un primo p^a son

$$1, p, p^2, \dots, p^a,$$

luego

$$\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} = \frac{p^{\alpha(a+1)} - 1}{p^\alpha - 1} \quad \text{si } \alpha \neq 0$$

$$= a + 1 \quad \text{si } \alpha = 0.$$

La inversa de Dirichlet de σ_α se puede expresar también como combinación lineal de las potencias α -ésimas de los divisores de n .

Teorema 2.20 Para $n \geq 1$ tenemos

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d) \mu\left(\frac{n}{d}\right).$$

DEMOSTRACIÓN. Puesto que $\sigma_\alpha = N^\alpha * u$ y N^α es completamente multiplicativa tenemos

$$\sigma_\alpha^{-1} = (\mu N^\alpha) * u^{-1} = (\mu N^\alpha) * \mu. \quad \square$$

2.14 CONVOLUCIONES GENERALIZADAS

A lo largo de esta sección F designa una función con valores reales o complejos definida en el eje real positivo $(0, \infty)$ tal que $F(x) = 0$ para $0 < x < 1$. Sumas del tipo

$$\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

son frecuentes en teoría de números. Aquí α es una función aritmética. La suma define una nueva función G en $(0, +\infty)$ que se anula también para $0 < x < 1$. Esta función G la designamos $\alpha \circ F$. Entonces

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Si $F(x) = 0$ para todo x no entero, la restricción de F a los enteros es una función aritmética y observamos que

$$(\alpha \circ F)(m) = (\alpha * F)(m)$$

para todo entero $m \geq 1$, por lo que la operación $\circ$ se puede considerar como una generalización de la convolución de Dirichlet $*$.

La operación $\circ$ en general, no es ni conmutativa, ni asociativa. Sin embargo, el teorema que sigue proporciona un sustituto útil de la ley asociativa.

Teorema 2.21 Propiedad asociativa que relaciona $\circ$ y $*$. Para todo par de funciones aritméticas α y β tenemos

$$(9) \quad \alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

DEMOSTRACIÓN. Para $x > 0$ tenemos

$$\begin{aligned} \{\alpha \circ (\beta \circ F)\}(x) &= \sum_{n \leq x} \alpha(n) \sum_{m \leq x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn \leq x} \alpha(n) \beta(m) F\left(\frac{x}{mn}\right) \\ &= \sum_{k \leq x} \left(\sum_{n|k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) = \sum_{k \leq x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\ &= \{(\alpha * \beta) \circ F\}(x). \end{aligned}$$

Esto termina la demostración. □

Observamos además que la función identidad $I(n) = [1/n]$ para la convolución de Dirichlet es también una identidad por la izquierda para la operación $\circ$. Es decir, tenemos

$$(I \circ F)(x) = \sum_{n \leq x} \left[\frac{1}{n} \right] F\left(\frac{x}{n}\right) = F(x).$$

Usamos ahora este resultado y la propiedad asociativa para demostrar la siguiente fórmula de inversión.

Teorema 2.22 Fórmula de inversión generalizada. Si α tiene inversa de Dirichlet α^{-1} , entonces la ecuación

$$(10) \quad G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

implica

$$(11) \quad F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right).$$

Recíprocamente, (11) implica (10).

DEMOSTRACIÓN. Si $G = \alpha \circ F$ entonces

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Entonces (10) implica (11). El recíproco se demuestra de forma análoga. □

El caso especial que sigue es particularmente importante.

Teorema 2.23 Fórmula de inversión de Möbius generalizada. Si α es completamente multiplicativa tenemos

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \quad \text{si, y sólo si,} \quad F(x) = \sum_{n \leq x} \mu(n) \alpha(n) G\left(\frac{x}{n}\right).$$

DEMOSTRACIÓN. En este caso $\alpha^{-1}(n) = \mu(n)\alpha(n)$. □

2.15 SERIES FORMALES DE POTENCIAS

En Cálculo, una serie infinita de la forma

$$(12) \quad \sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \cdots$$

se llama serie de potencias en x . Tanto x como los coeficientes $a(n)$ son números reales o complejos. A cada serie de potencias le corresponde un radio de convergencia $r \geq 0$ tal que la serie converge absolutamente si $|x| < r$ y diverge si $|x| > r$. (El radio r puede ser $+\infty$).

En esta sección consideraremos series de potencias desde un punto de vista distinto. Las llamaremos series *formales* de potencias para distinguirlas de las series de potencias ordinarias del Análisis. En la teoría de las series formales de potencias a x no se le asigna valor numérico alguno, y las cuestiones acerca de la convergencia y la divergencia carecen de interés.

El objeto de interés lo constituye la sucesión de los coeficientes

$$(13) \quad (a(0), a(1), \dots, a(n), \dots).$$

Todo lo que obtengamos con series formales de potencias lo podríamos obtener también estudiando la sucesión de los coeficientes como un vector infinito-dimensional de componentes $a(0), a(1), \dots$. Pero para nuestros propósitos es más conveniente considerar los términos como coeficientes de una serie de potencias como en (12) que como componentes de un vector como en (13). El símbolo x^n es simplemente una marca para localizar la posición del coeficiente n -ésimo $a(n)$. El coeficiente $a(0)$ se llama *coeficiente constante* de la serie.

Operamos las series formales de potencias algebraicamente como si pensásemos que son series de potencias convergentes. Si $A(x)$ y $B(x)$ son dos series formales de potencias, por ejemplo

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \quad \text{y} \quad B(x) = \sum_{n=0}^{\infty} b(n)x^n,$$

definimos

Igualdad: $A(x) = B(x)$ significa que $a(n) = b(n)$ para todo $n \geq 0$.

Suma: $A(x) + B(x) = \sum_{n=0}^{\infty} (a(n) + b(n))x^n$.

Producto: $A(x)B(x) = \sum_{n=0}^{\infty} c(n)x^n$, en donde

$$(14) \quad c(n) = \sum_{k=0}^n a(k)b(n-k).$$

La sucesión $\{c(n)\}$ determinada por (14) se llama *producto de Cauchy* de las sucesiones $\{a(n)\}$ y $\{b(n)\}$.

El lector puede comprobar con facilidad que estas dos operaciones satisfacen las propiedades conmutativa y asociativa, y que la multiplicación es distributiva respecto de la suma. En el lenguaje de la Álgebra moderna, las series formales de potencias constituyen un *anillo*. Este anillo posee un *elemento cero* para la suma que designaremos por 0,

$$0 = \sum_{n=0}^{\infty} a(n)x^n, \quad \text{en donde } a(n) = 0 \text{ para todo } n \geq 0,$$

y un *elemento identidad* para la multiplicación que designaremos por 1,

$$1 = \sum_{n=0}^{\infty} a(n)x^n, \quad \text{en donde } a(0) = 1 \text{ y } a(n) = 0 \text{ para } n \geq 1.$$

Una serie formal de potencias se llama un *polinomio formal* si todos sus coeficientes son 0 a partir de un lugar en adelante.

Para cada serie formal de potencias $A(x) = \sum_{n=0}^{\infty} a(n)x^n$ con coeficiente constante $a(0) \neq 0$ existe una serie formal de potencias unívocamente determinada $B(x) = \sum_{n=0}^{\infty} b(n)x^n$ tal que $A(x)B(x) = 1$. Sus coeficientes se pueden determinar resolviendo el sistema infinito de ecuaciones

$$\begin{aligned} a(0)b(0) &= 1 \\ a(0)b(1) + a(1)b(0) &= 0, \\ a(0)b(2) + a(1)b(1) + a(2)b(0) &= 0, \\ &\vdots \end{aligned}$$

sucesivamente para $b(0), b(1), b(2), \dots$. La serie $B(x)$ se llama *inversa de $A(x)$* y se designa por $A(x)^{-1}$ o por $1/A(x)$.

La serie especial

$$A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n$$

se llama *serie geométrica*. Aquí a es un número real o complejo arbitrario. Su inversa es el polinomio formal

$$B(x) = 1 - ax.$$

En otras palabras tenemos

$$\frac{1}{1 - ax} = 1 + \sum_{n=1}^{\infty} a^n x^n.$$

2.16 LA SERIE DE BELL DE UNA FUNCIÓN ARITMÉTICA

E. T. Bell utilizó series formales de potencias para estudiar las propiedades de las funciones aritméticas multiplicativas.

Definición. Dada una función aritmética f y un primo p , designamos por $f_p(x)$ a la serie formal de potencias

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n)x^n$$

y la llamamos serie de Bell de f módulo p .

Las series de Bell son especialmente útiles cuando f es multiplicativa.

Teorema 2.24 Teorema de unicidad. Sean f y g funciones multiplicativas. Entonces $f = g$ si, y sólo si

$$f_p(x) = g_p(x) \quad \text{para todo primo } p.$$

DEMOSTRACIÓN. Si $f = g$ entonces $f(p^n) = g(p^n)$ para todo p y todo $n \geq 0$, luego $f_p(x) = g_p(x)$. Recíprocamente, si $f_p(x) = g_p(x)$ para todo p entonces $f(p^n) = g(p^n)$ para todo $n \geq 0$. Dado que f y g son multiplicativas y coinciden sobre todas las potencias de primos coinciden sobre todos los números enteros positivos, luego $f = g$. $\square$

Es fácil determinar la serie de Bell para algunas de las funciones multiplicativas introducidas con anterioridad en este capítulo.

EJEMPLO 1 Función de Möbius μ . Puesto que $\mu(p) = -1$ y $\mu(p^n) = 0$ para $n \geq 2$ tenemos

$$\mu_p(x) = 1 - x.$$

EJEMPLO 2 Indicatriz de Euler φ . Dado que $\varphi(p^n) = p^n - p^{n-1}$ para $n \geq 1$ tenemos

$$\begin{aligned} \varphi_p(x) &= 1 + \sum_{n=1}^{\infty} (p^n - p^{n-1})x^n = \sum_{n=0}^{\infty} p^n x^n - x \sum_{n=0}^{\infty} p^n x^n \\ &= (1 - x) \sum_{n=0}^{\infty} p^n x^n = \frac{1 - x}{1 - px}. \end{aligned}$$

EJEMPLO 3. Funciones completamente multiplicativas. Si f es completamente multiplicativa, entonces $f(p^n) = f(p)^n$ para todo $n \geq 0$ por lo tanto la serie de Bell $f_p(x)$ es una serie geométrica,

$$f_p(x) = \sum_{n=0}^{\infty} f(p)^n x^n = \frac{1}{1 - f(p)x}.$$

En particular tenemos las siguientes series de Bell para la función identidad I , la función unidad u , la función de potencia N^α y la función de Liouville λ :

$$I_p(x) = 1.$$

$$u_p(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1 - x}.$$

$$N_p^\alpha(x) = 1 + \sum_{n=1}^{\infty} p^{\alpha n} x^n = \frac{1}{1 - p^\alpha x}.$$

$$\lambda_p(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1 + x}.$$

2.17 SERIES DE BELL Y PRODUCTO DE DIRICHLET

El teorema que sigue relaciona la multiplicación de series de Bell con la multiplicación de Dirichlet.

Teorema 2.25 *Para todo par de funciones aritméticas f y g , sea $h = f * g$. Entonces para cada primo p tenemos*

$$h_p(x) = f_p(x)g_p(x).$$

DEMOSTRACIÓN. Puesto que los divisores de p^n son $1, p, p^2, \dots, p^n$ tenemos

$$h(p^n) = \sum_{d|p^n} f(d)g\left(\frac{p^n}{d}\right) = \sum_{k=0}^n f(p^k)g(p^{n-k}).$$

Esto completa la demostración puesto que la última suma es el producto de Cauchy de las sucesiones $\{f(p^n)\}$ y $\{g(p^n)\}$. $\square$

EJEMPLO 1 Puesto que $\mu^2(n) = \lambda^{-1}(n)$ la serie de Bell de μ^2 módulo p es

$$\mu_p^2(x) = \frac{1}{\lambda_p(x)} = 1 + x.$$

EJEMPLO 2 Puesto que $\sigma_a = N^a * u$ la serie de Bell de σ_a módulo p es

$$(\sigma_a)_p(x) = N_p^a(x)u_p(x) = \frac{1}{1 - p^a x} \cdot \frac{1}{1 - x} = \frac{1}{1 - \sigma_a(p)x + p^a x^2}.$$

EJEMPLO 3 Este ejemplo ilustra cómo podemos utilizar las series de Bell para obtener ecuaciones entre funciones aritméticas. Sea

$$f(n) = 2^{v(n)},$$

en donde $v(1) = 0$ y $v(n) = k$ si $n = p_1^{a_1} \dots p_k^{a_k}$. Entonces f es multiplicativa y su serie de Bell módulo p es

$$f_p(x) = 1 + \sum_{n=1}^{\infty} 2^{v(p^n)} x^n = 1 + \sum_{n=1}^{\infty} 2x^n = 1 + \frac{2x}{1-x} = \frac{1+x}{1-x}.$$

Por lo tanto

$$f_p(x) = \mu_p^2(x)u_p(x)$$

que implica $f = \mu^2 * u$, o

$$2^{v(n)} = \sum_{d|n} \mu^2(d).$$

2.18 DERIVADAS DE FUNCIONES ARITMÉTICAS

Definición. Para toda función aritmética f definimos su derivada f' como la función aritmética dada por la ecuación

$$f'(n) = f(n)\log n \quad \text{para } n \geq 1.$$

EJEMPLOS Puesto que $I(n)\log n = 0$ para todo n tenemos $I' = 0$. Dado que $u(n) = 1$ para todo n tenemos $u'(n) = \log n$. Por lo tanto, la fórmula $\sum_{d|n} \Lambda(d) = \log n$ se puede escribir

$$(15) \quad \Lambda * u = u'.$$

Este concepto de derivada posee muchas de las propiedades de la derivada usual estudiada en Análisis elemental. Por ejemplo, las reglas usuales para derivar sumas y productos se conservan si los productos son productos de Dirichlet.

Teorema 2.26 Si f y g son funciones aritméticas tenemos:

- (a) $(f + g)' = f' + g'$.
- (b) $(f * g)' = f' * g + f * g'$.
- (c) $(f^{-1})' = -f' * (f * f)^{-1}$, si $f(1) \neq 0$.

DEMOSTRACIÓN. La demostración de (a) es inmediata. Además, es sabido que $f + g$ es la función tal que, para todo n , $(f + g)(n) = f(n) + g(n)$.

Para probar (b) utilizamos la identidad $\log n = \log d + \log(n/d)$ para escribir

$$\begin{aligned} (f * g)'(n) &= \sum_{d|n} f(d)g\left(\frac{n}{d}\right)\log n \\ &= \sum_{d|n} f(d)\log d g\left(\frac{n}{d}\right) + \sum_{d|n} f(d)g\left(\frac{n}{d}\right)\log\left(\frac{n}{d}\right) \\ &= (f' * g)(n) + (f * g')(n). \end{aligned}$$

Para probar (c) aplicamos la parte (b) a la fórmula $I' = 0$, recordando que $I = f * f^{-1}$. Esto nos proporciona

$$0 = (f * f^{-1})' = f' * f^{-1} + f * (f^{-1})'$$

luego

$$f * (f^{-1})' = -f' * f^{-1}.$$

Multiplicando por f^{-1} obtenemos

$$(f^{-1})' = -(f' * f^{-1}) * f^{-1} = -f' * (f^{-1} * f^{-1}).$$

Pero $f^{-1} * f^{-1} = (f * f)^{-1}$, por lo tanto (c) queda demostrado. $\square$

2.19 LA IDENTIDAD DE SELBERG

Utilizando el concepto de derivada podemos obtener rápidamente una fórmula de Selberg que se utiliza a menudo como punto de partida de una demostración elemental del teorema del número primo.

Teorema 2.27 La identidad de Selberg. *Para $n \geq 1$ tenemos*

$$\Lambda(n) \log n + \sum_{d|n} \Lambda(d) \Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \log^2 \frac{n}{d}.$$

DEMOSTRACIÓN. La ecuación (15) establece que $\Lambda * u = u'$. La diferenciación de esta ecuación nos proporciona

$$\Lambda' * u + \Lambda * u' = u''$$

luego, puesto que $u' = \Lambda * u$,

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

Ahora multiplicamos ambos miembros por $\mu = u^{-1}$ y obtenemos

$$\Lambda' + \Lambda * \Lambda = u'' * \mu.$$

Esta es la identidad requerida. $\square$

Ejercicios del capítulo 2

1. Buscar todos los enteros n tales que

$$(a) \varphi(n) = n/2, \quad (b) \varphi(n) = \varphi(2n), \quad (c) \varphi(n) = 12.$$

2. Para cada una de las proposiciones que siguen establecer una demostración o presentar un contraejemplo.

- (a) Si $(m, n) = 1$ entonces $(\varphi(m), \varphi(n)) = 1$.
 (b) Si n es compuesto, entonces $(n, \varphi(n)) > 1$.
 (c) Si los mismos primos dividen a m y a n , entonces $n\varphi(m) = m\varphi(n)$.

3. Probar que

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}.$$

4. Probar que $\varphi(n) > n/6$ para todo n con 8 factores primos distintos, como máximo.
 5. Definimos $v(1) = 0$ y, para $n > 1$, $v(n)$ es el número de factores primos distintos de n .
 Sea $f = \mu * v$ y demostrar que $f(n)$ es 0 ó 1.
 6. Probar que

$$\sum_{d^2|n} \mu(d) = \mu^2(n)$$

y, en general,

$$\sum_{d^k|n} \mu(d) = \begin{cases} 0 & \text{si } m^k | n \text{ para algún } m < 1, \\ 1 & \text{en otro caso} \end{cases}$$

La última suma se extiende a todos los divisores positivos d de n cuya potencia k -ésima también divide a n .

7. Si $\mu(p, d)$ denota el valor de la función de Möbius en el mcd de p y d , probar que, para cada primo p , tenemos

$$\sum_{d|n} \mu(d) \mu(p, d) = \begin{cases} 1 & \text{si } n = 1, \\ 2 & \text{si } n = p^a, a \geq 1, \\ 0 & \text{en otro caso.} \end{cases}$$

8. Probar que

$$\sum_{d|n} \mu(d) \log^m d = 0$$

si $m \geq 1$ y n posee más de m factores primos distintos. [Indicación: Inducción.]

9. Si x es real, $x \geq 1$, y $\varphi(x, n)$ designa el número de enteros positivos $\leq x$ que son primos con n . [Obsérvese que $\varphi(n, n) = \varphi(n)$.] Probar que

$$\varphi(x, n) = \sum_{d|n} \mu(d) \left[\frac{x}{d} \right] \quad \text{y} \quad \sum_{d|n} \varphi\left(\frac{x}{d}, \frac{n}{d}\right) = [x].$$

En los ejercicios 10, 11 y 12, $d(n)$ designa el número de divisores positivos de n .

10. Probar que $\prod_{t|n} t = n^{d(n)/2}$.
11. Probar que $d(n)$ es impar si, y sólo si, n es un cuadrado.
12. Probar que $\sum_{t|n} d(t)^3 = (\sum_{t|n} d(t))^2$.
13. Forma producto de la fórmula de inversión de Möbius. Si $f(n) < 0$ para todo n y si $a(n)$ es real, $a(1) \neq 0$, probar que

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \text{ si, y sólo si, } f(n) = \prod_{d|n} g(d)^{b(n/d)},$$

en donde $b = a^{-1}$ es la inversa de Dirichlet de a .

14. Sea $f(x)$ definida para todo racional x de $0 \leq x \leq 1$ y sea

$$F(n) = \sum_{k=1}^n f\left(\frac{k}{n}\right), \quad F^*(n) = \sum_{\substack{k=1 \\ (k, n)=1}}^n f\left(\frac{k}{n}\right).$$

- (a) Probar que $F^* = \mu * F$, producto de Dirichlet de μ y F .
- (b) Utilizar (a) o algún otro método para probar que $\mu(n)$ es la suma de las raíces n -ésimas primitivas de la unidad:

$$\mu(n) = \sum_{\substack{k=1 \\ (k, n)=1}}^n e^{2\pi i k/n}.$$

15. Sea $\varphi_k(n)$ la suma de las potencias de orden k de los números $\leq n$ y primos con n . Obsérvese que $\varphi_0(n) = \varphi(n)$. Usar el ejercicio 14 u otro método para probar que

$$\sum_{d|n} \frac{\varphi_k(d)}{d^k} = \frac{1^k + \cdots + n^k}{n^k}.$$

16. Invertir la fórmula del ejercicio 15 a fin de obtener, para $n > 1$,

$$\varphi_1(n) = \frac{1}{2} n \varphi(n), \quad \text{y} \quad \varphi_2(n) = \frac{1}{3} n^2 \varphi(n) + \frac{n}{6} \prod_{p|n} (1-p).$$

Deducir una fórmula que corresponda a $\varphi_3(n)$.

17. La indicatriz de Jordan J_k es una generalización de la indicatriz de Euler definida por

$$J_k(n) = n^k \prod_{p|n} (1 - p^{-k}).$$

(a) Probar que

$$J_k(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k \quad \text{y} \quad n^k = \sum_{d|n} J_k(d).$$

(b) Determinar la serie de Bell de J_k .

18. Probar que cada número de la forma $2^{a-1}(2^a - 1)$ es perfecto si $2^a - 1$ es primo.

19. Probar que si n es par y perfecto entonces $n = 2^{a-1}(2^a - 1)$ para un $a \geq 2$. No sabemos si existen números impares perfectos. Sabemos que no existen impares perfectos con menos de 7 factores primos.

20. Sea $P(n)$ el producto de los enteros positivos que son $\leq n$ y primos con n . Probar que

$$P(n) = n^{\varphi(n)} \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)}$$

21. Sea $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$. Probar que f es multiplicativa pero no es completamente multiplicativa.

22. Probar que

$$\sigma_1(n) = \sum_{d|n} \varphi(d) \sigma_0\left(\frac{n}{d}\right),$$

y deducir una generalización que contenga $\sigma_a(n)$. (Es posible más de una generalización.)

23. Probar la proposición que sigue o dar un contraejemplo. Si f es multiplicativa, entonces $F(n) = \prod_{d|n} f(d)$ es multiplicativa.

24. Sean $A(x)$ y $B(x)$ dos series formales de potencias. Si el producto $A(x)B(x)$ es la serie nula, probar que uno de los factores, por lo menos, es la serie nula. En otras palabras, el anillo de las series formales de potencias carece de divisores de cero.
25. Suponemos que f es multiplicativa. Probar que:

- (a) $f^{-1}(n) = \varphi(n)f(n)$ para cada n carente de cuadrados.
 (b) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ para cada primo p .

26. Suponemos que f es multiplicativa. Probar que f es completamente multiplicativa si, y sólo si, $f^{-1}(p^a) = 0$ para todo primo p y todo entero $a \geq 2$.
27. (a) Si f es completamente multiplicativa, probar que, para todo par de funciones aritméticas g y h ,

$$f \cdot (g * h) = (f \cdot g) * (f \cdot h)$$

en donde $f \cdot g$ designa el producto ordinario, $(f \cdot g)(n) = f(n)g(n)$.

(b) Si f es multiplicativa y si la relación dada en (a) se verifica para $g = \mu$ y $h = \mu^{-1}$, probar que f es completamente multiplicativa.

28. (a) Si f es completamente multiplicativa, probar que

$$(f \cdot g)^{-1} = f \cdot g^{-1}$$

para cada función aritmética g con $g(1) \neq 0$.

(b) Si f es multiplicativa y la relación dada en (a) se verifica para $g = \mu^{-1}$, probar que f es completamente multiplicativa.

29. Probar que existe una función aritmética multiplicativa g tal que

$$\sum_{k=1}^n f((k, n)) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

para cada función aritmética f . Aquí (k, n) es el mcd de n y k . Utilizar esta identidad para probar que

$$\sum_{k=1}^n (k, n)\mu((k, n)) = \mu(n).$$

30. Sea f una función multiplicativa y sea g una función aritmética. Suponemos que

$$(a) \quad f(p^{n+1}) = f(p)f(p^n) - g(p)f(p^{n-1}) \quad \text{para todos los primos } p \text{ y todo } n \geq 1.$$

Probar que, para cada primo p , la serie de Bell de f tiene la forma

$$(b) \quad f_p(x) = \frac{1}{1 - f(p)x + g(p)x^2}.$$

Recíprocamente, probar que (b) implica (a).

31. (Continuación del ejercicio 30.) Si g es completamente multiplicativa demostrar que la proposición (a) del ejercicio 30 implica

$$f(m)f(n) = \sum_{d|(m,n)} g(d)f\left(\frac{mn}{d^2}\right),$$

en donde la suma se halla extendida a los divisores positivos del mcd (m, n) . [Indicación: Considerar en primer lugar el caso $m = p^a$, $n = p^b$.]

32. Probar que

$$\sigma_a(m)\sigma_a(n) = \sum_{d|(m,n)} d^a \sigma_a\left(\frac{mn}{d^2}\right).$$

33. Probar que la función de Liouville viene dada por la fórmula

$$\lambda(n) = \sum_{d^2|n} \mu\left(\frac{n}{d^2}\right).$$

34. Este ejercicio describe otra demostración del teorema 2.16 que establece que la inversa de Dirichlet de una función multiplicativa es multiplicativa. Suponemos que g es multiplicativa y hacemos $f = g^{-1}$.

- (a) Probar que, si p es primo, entonces para $k \geq 1$ tenemos

$$f(p^k) = - \sum_{i=1}^k g(p^i) f(p^{k-i}).$$

- (b) Sea h la función multiplicativa unívocamente determinada que coincide con f en las potencias de primos. Probar que $h * g$ coincide con la función identidad I en las potencias de primos y deducir que $h * g = I$. Ello demuestra que $f = h$, luego f es multiplicativa.

35. Si f y g son multiplicativas y, a y b son enteros positivos con $a \geq b$, probar que la función h dada por

$$h(n) = \sum_{d^a|n} f\left(\frac{n}{d^a}\right) g\left(\frac{n}{d^b}\right)$$

también es multiplicativa. La suma se halla extendida a los divisores d de n tales que d^a divide a n .

FUNCIONES DE MÖBIUS DE ORDEN k .

Si $k \geq 1$ definimos μ_k , la función de Möbius de orden k , como sigue:

$$\begin{aligned}\mu_k(1) &= 1, \\ \mu_k(n) &= 0 \text{ si } p^{k+1} | n \text{ para algún primo } p, \\ \mu_k(n) &= (-1)^r \text{ si } n = p_1^{a_1} \cdots p_r^{a_r} \prod_{i>r} p_i^{a_i}, \quad 0 \leq a_i < k, \\ \mu_k(n) &= 1 \text{ en otro caso.}\end{aligned}$$

En otras palabras, $\mu_k(n)$ se anula si n es divisible por la potencia de exponente $(k+1)$ de algún primo; en otras palabras, $\mu_k(n)$ es 1 salvo en el caso en que la descomposición en factores primos de n contiene las potencias de exponente k de r primos distintos, exactamente, en cuyo caso $\mu_k(n) = (-1)^r$. Obsérvese que $\mu_1 = \mu$, función usual de Möbius.

Probar las propiedades de las funciones μ_k de Möbius descritas en los siguientes ejercicios.

36. Si $k \geq 1$, entonces $\mu_k(n^k) = \mu(n)$.
37. Cada función μ_k es multiplicativa.
38. Si $k \geq 2$ tenemos

$$\mu_k(n) = \sum_{d^k | n} \mu_{k-1}\left(\frac{n}{d^k}\right) \mu_{k-1}\left(\frac{n}{d}\right).$$

38. Si $k \geq 1$ tenemos

$$|\mu_k(n)| = \sum_{d^{k+1} | n} \mu(d).$$

40. Para cada primo p la serie de Bell de μ_k viene dada por

$$(\mu_k)_p(x) = \frac{1 - 2x^k + x^{k+1}}{1 - x}.$$

Capítulo 3

Medias de funciones aritméticas

3.1 INTRODUCCIÓN

En el último capítulo hemos analizado varias identidades satisfechas por las funciones aritméticas $\mu(n)$, $\varphi(n)$, $\Lambda(n)$, y por las funciones divisor $\sigma_a(n)$. Ahora nos preguntamos acerca del comportamiento de estas y otras funciones aritméticas $f(n)$ para valores grandes de n .

Por ejemplo, consideramos $d(n)$, número de divisores de n . Esta función toma el valor 2 una infinidad de veces (cuando n es primo) y también toma valores grandes cuando n posee un número grande de divisores. Por lo tanto los valores de $d(n)$ fluctúan considerablemente cuando n crece.

Muchas de las funciones aritméticas fluctúan de esta forma y, a menudo, es difícil determinar su comportamiento para n grande. A veces es mucho más fructífera su media aritmética

$$\tilde{f}(n) = \frac{1}{n} \sum_{k=1}^n f(k).$$

Las medias suavizan las fluctuaciones de forma que resulta razonable esperar que los valores medios $\tilde{f}(n)$ poseen un comportamiento más regular que $f(n)$. Esto es así para el caso de la función divisor $d(n)$. Más adelante probaremos que la media $\tilde{d}(n)$ se comporta como $\log n$ para n suficientemente grande; precisando

$$(1) \quad \lim_{n \rightarrow \infty} \frac{\tilde{d}(n)}{\log n} = 1.$$

Esto se expresa diciendo que el orden medio de $d(n)$ es $\log n$.

Para estudiar la media de una función arbitraria f necesitamos un cierto conocimiento de sus sumas parciales $\sum_{k=1}^n f(k)$. A veces es conveniente reemplazar el índice superior n por un número real positivo x arbitrario y considerar en su lugar sumas de la forma

$$\sum_{k \leq x} f(k).$$

Entendemos entonces que los índices k varían de 1 a $[x]$, el mayor entero $\leq x$. Si $0 < x < 1$ la suma es vacía y le asignamos el valor 0. Nuestro propósito consiste en determinar el comportamiento de esta suma en función de x , especialmente para x grande.

Para la función divisor probaremos un resultado obtenido por Dirichlet en 1849, más fuerte que (1), a saber

$$(2) \quad \sum_{k \leq x} d(k) = x \log x + (2C - 1)x + O(\sqrt{x})$$

para todo $x \geq 1$. Aquí C es la constante de Euler definida por la ecuación

$$(3) \quad C = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \right).$$

El símbolo $O(\sqrt{x})$ representa una función no especificada de x que se halla dominada por un número constante de veces $\sqrt{x}$. Este resultado constituye un ejemplo de la notación «O mayúscula» que se define como sigue:

3.2 LA NOTACIÓN O MAYÚSCULA. IGUALDAD ASINTÓTICA DE FUNCIONES

Definición. Si $g(x) > 0$ para todo $x \geq a$, escribiremos

$$f(x) = O(g(x)) \quad (\text{léase: «}f(x)\text{ es O mayúscula de }g(x)\text{»})$$

para indicar que el cociente $f(x)/g(x)$ se halla acotado para $x \geq a$; esto es, existe una constante $M > 0$ tal que

$$|f(x)| \leq Mg(x) \quad \text{para todo } x \geq a.$$

Una ecuación de la forma

$$f(x) = h(x) + O(g(x))$$

significa que $f(x) - h(x) = O(g(x))$. Observemos que $f(t) = O(g(t))$ para $t \geq a$ implica $\int_a^x f(t)dt = O(\int_a^x g(t)dt)$ para $x \geq a$.

Definición. Si

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$$

diremos que $f(x)$ es asintótica a $g(x)$ cuando $x \rightarrow \infty$, y escribiremos

$$f(x) \sim g(x) \quad \text{cuando } x \rightarrow \infty.$$

Por ejemplo, la ecuación (2) implica que

$$\sum_{k \leq x} d(k) \sim x \log x \quad \text{cuando } x \rightarrow \infty.$$

En la ecuación (2) el término $x \log x$ se llama el valor asintótico de la suma; los otros dos términos representan el error cometido al aproximar la suma por medio de su valor asintótico. Si este error lo designamos por $E(x)$, entonces (2) establece que

$$(4) \quad E(x) = (2C - 1)x + O(\sqrt{x}).$$

Esto podría escribirse también $E(x) = O(x)$, ecuación que sería correcta si bien no nos comunica la información más precisa contenida en (4). La ecuación (4) nos dice que el valor asintótico de $E(x)$ es $(2C - 1)x$.

3.3 FÓRMULA DE SUMACIÓN DE EULER

A veces los valores asintóticos de una suma parcial se pueden obtener comparándola con una integral. Una fórmula de sumación de Euler da una expresión

exacta del error cometido en tales aproximaciones. En esta fórmula $[t]$ designa el mayor entero $\leq t$.

Teorema 3.1 Fórmula de sumación de Euler. Si f posee derivada continua f' en el intervalo $[y, x]$, en donde $0 < y < x$, entonces

$$(5) \quad \sum_{y < n \leq x} f(n) = \int_y^x f(t) dt + \int_y^x (t - [t])f'(t) dt \\ + f(x)([x] - x) - f(y)([y] - y).$$

DEMOSTRACIÓN. Sea $m = [y]$, $k = [x]$. Para enteros n y $n - 1$ de $[y, x]$ tenemos

$$\int_{n-1}^n [t]f'(t) dt = \int_{n-1}^n (n-1)f'(t) dt = (n-1)\{f(n) - f(n-1)\} \\ = \{nf(n) - (n-1)f(n-1)\} - f(n).$$

Si sumamos desde $n = m + 1$ hasta $n = k$ obtenemos

$$\int_m^k [t]f'(t) dt = \sum_{n=m+1}^k \{nf(n) - (n-1)f(n-1)\} - \sum_{y < n \leq x} f(n) \\ = kf(k) - mf(m) - \sum_{y < n \leq x} f(n),$$

por lo tanto

$$(6) \quad \sum_{y < n \leq x} f(n) = - \int_m^k [t]f'(t) dt + kf(k) - mf(m) \\ = - \int_y^x [t]f'(t) dt + kf(x) - mf(y).$$

La integración por partes nos da

$$\int_y^x f(t) dt = xf(x) - yf(y) - \int_y^x tf'(t) dt,$$

y al combinar este resultado con (6) obtenemos (5). □

3.4 ALGUNAS FÓRMULAS ASINTÓTICAS ELEMENTALES

El teorema que sigue proporciona un número de fórmulas asintóticas que son consecuencias fáciles de la fórmula de sumación de Euler. En la parte (a) la constante C es la constante de Euler definida en (3). En la parte (b), $\zeta(s)$ designa la función zeta de Riemann que se define por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{si } s > 1,$$

y por la ecuación

$$\zeta(s) = \lim_{x \rightarrow \infty} \left(\sum_{n \leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right) \quad \text{si } 0 < s < 1.$$

Teorema 3.2 Si $x \geq 1$ tenemos:

- (a) $\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right).$
- (b) $\sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}) \quad \text{si } s > 0, s \neq 1.$
- (c) $\sum_{n > x} \frac{1}{n^s} = O(x^{1-s}) \quad \text{si } s > 1.$
- (d) $\sum_{n \leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha) \quad \text{si } \alpha \geq 0.$

DEMOSTRACIÓN. Para la parte (a) tomamos $f(t) = 1/t$ en la fórmula de sumación de Euler para obtener

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t - [t]}{t^2} dt + 1 - \frac{x - [x]}{x} \\ &= \log x - \int_1^x \frac{t - [t]}{t^2} dt + 1 + O\left(\frac{1}{x}\right) \\ &= \log x + 1 - \int_1^\infty \frac{t - [t]}{t^2} dt + \int_x^\infty \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right). \end{aligned}$$

La integral impropia $\int_1^\infty (t - [t])t^{-2} dt$ existe puesto que está dominada por $\int_1^\infty t^{-2} dt$. Además,

$$0 \leq \int_x^\infty \frac{t - [t]}{t^2} dt \leq \int_x^\infty \frac{1}{t^2} dt = \frac{1}{x}$$

luego la última ecuación conduce a

$$\sum_{n \leq x} \frac{1}{n} = \log x + 1 - \int_1^\infty \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right).$$

Esto demuestra (a) con

$$C = 1 - \int_1^\infty \frac{t - [t]}{t^2} dt.$$

Si hacemos que $x \rightarrow \infty$ en (a) obtenemos que

$$\lim_{x \rightarrow \infty} \left(\sum_{n \leq x} \frac{1}{n} - \log x \right) = 1 - \int_1^\infty \frac{t - [t]}{t^2} dt,$$

luego C es igual a la constante de Euler.

Para probar (b) utilizamos el mismo tipo de argumento con $f(x) = x^{-s}$, en donde $s > 0$, $s \neq 1$. La fórmula de sumación de Euler nos proporciona

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n^s} &= \int_1^x \frac{dt}{t^s} - s \int_1^x \frac{t - [t]}{t^{s+1}} dt + 1 - \frac{x - [x]}{x^s} \\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s \int_1^\infty \frac{t - [t]}{t^{s+1}} dt + O(x^{-s}). \end{aligned}$$

Por consiguiente

$$(7) \quad \sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s}),$$

en donde

$$C(s) = 1 - \frac{1}{1-s} - s \int_1^\infty \frac{t - [t]}{t^{s+1}} dt.$$

Si $s < 1$, el primer miembro de (7) tiende a $\zeta(s)$ cuando $x \rightarrow \infty$ y los términos x^{1-s} y x^{-s} tienden ambos a 0. Por lo tanto $C(s) = \zeta(s)$ si $s < 1$. Si $0 < s < 1$, $x^{-s} \rightarrow 0$ y (7) prueba que

$$\lim_{x \rightarrow \infty} \left(\sum_{n \leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right) = C(s).$$

Por lo tanto, $C(s)$ es también igual a $\zeta(s)$ si $0 < s < 1$. Esto demuestra (b).

Para demostrar (c) usamos (b) con $s > 1$ a fin de obtener

$$\sum_{n > x} \frac{1}{n^s} = \zeta(s) - \sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{s-1} + O(x^{-s}) = O(x^{1-s})$$

ya que $x^{-s} \leq x^{1-s}$.

Finalmente, para demostrar (d) utilizamos una vez más la fórmula de sumación de Euler con $f(t) = t^\alpha$ para obtener

$$\begin{aligned} \sum_{n \leq x} n^\alpha &= \int_1^x t^\alpha dt + \alpha \int_1^x t^{\alpha-1} (t - [t]) dt + 1 - (x - [x])x^\alpha \\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha \int_1^x t^{\alpha-1} dt\right) + O(x^\alpha) \\ &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha). \end{aligned}$$

□

3.5 EL ORDEN MEDIO DE $d(n)$

En esta sección obtenemos fórmulas asintóticas de Dirichlet para las sumas parciales de la función divisor $d(n)$.

Teorema 3.3 Para todo $x \geq 1$ tenemos

$$(8) \quad \sum_{n \leq x} d(n) = x \log x + (2C - 1)x + O(\sqrt{x}),$$

en donde C es la constante de Euler.

DEMOSTRACIÓN. Puesto que $d(n) = \sum_{d|n} 1$ tenemos

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{d|n} 1.$$

Esta es una suma doble extendida a n y a d . Puesto que $d|n$ podemos escribir $n = qd$ y extender la suma a todos los pares de enteros positivos q, d con $qd \leq x$. Luego,

$$(9) \quad \sum_{n \leq x} d(n) = \sum_{\substack{q, d \\ qd \leq x}} 1.$$

Esto se puede interpretar como una suma extendida a ciertos puntos reticulares del plano qd , tal como sugiere la figura 3.1. (Un punto reticular es un punto de coordenadas enteras.) Los puntos reticulares con $qd = n$ pertenecen a una hipérbola. luego la suma de (9) cuenta el número de puntos reticulares que se hallan sobre las hipérbolas que corresponden a $n = 1, 2, \dots, [x]$. Para cada d fijo $\leq x$ podemos contar en primer lugar los puntos reticulares que se hallan en el segmento rectilíneo horizontal $1 \leq q \leq x/d$, y sumar después para todos los $d \leq x$. Con lo que (9) se transforma en

$$(10) \quad \sum_{n \leq x} d(n) = \sum_{d \leq x} \sum_{q \leq x/d} 1.$$

Ahora utilizamos la parte (d) del teorema 3.2 con $\alpha = 0$ a fin de obtener

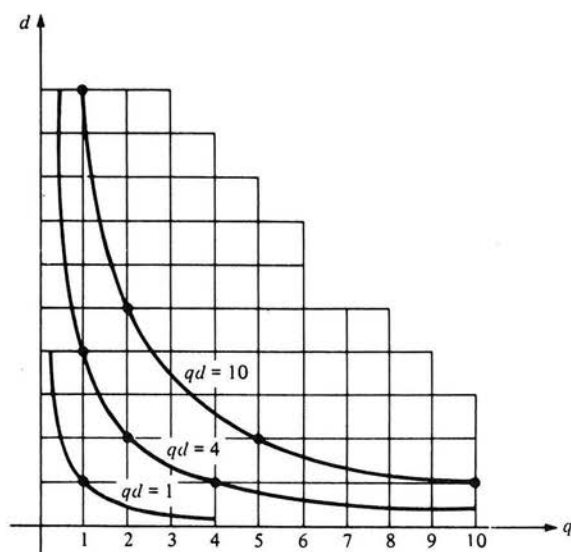


Figura 3.1

$$\sum_{q \leq x/d} 1 = \frac{x}{d} + O(1).$$

Utilizando este resultado junto con el teorema 3.2(a) obtenemos

$$\begin{aligned} \sum_{n \leq x} d(n) &= \sum_{d \leq x} \left\{ \frac{x}{d} + O(1) \right\} = x \sum_{d \leq x} \frac{1}{d} + O(x) \\ &= x \left\{ \log x + C + O\left(\frac{1}{x}\right) \right\} + O(x) = x \log x + O(x). \end{aligned}$$

Este resultado constituye una versión débil de (8) que implica

$$\sum_{n \leq x} d(n) \sim x \log x \quad \text{cuando } x \rightarrow \infty$$

y da $\log n$ como el orden medio de $d(n)$.

Para probar la fórmula más precisa (8) volvemos a la suma (9) que cuenta el número de puntos reticulares que se hallan en una región hiperbólica y saca ven-

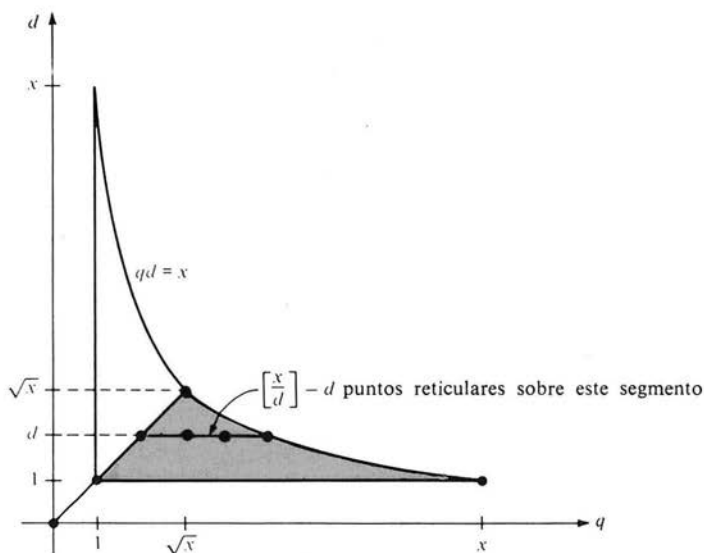


Figura 3.2

taja de la simetría de la región respecto de la recta $q = d$. El número total de puntos reticulares que se hallan en la región es igual a dos veces el número que se hallan debajo de la recta $q = d$ más el número de puntos que se hallan en el segmento rectilíneo bisectriz. Refiriéndonos a la figura 3.2 vemos que

$$\sum_{n \leq x} d(n) = 2 \sum_{d \leq \sqrt{x}} \left\{ \left\lfloor \frac{x}{d} \right\rfloor - d \right\} + [\sqrt{x}].$$

Usamos ahora la relación $[y] = y + O(1)$ y las partes (a) y (d) del teorema 3.2 para obtener

$$\begin{aligned} \sum_{n \leq x} d(n) &= 2 \sum_{d \leq \sqrt{x}} \left\{ \frac{x}{d} - d + O(1) \right\} + O(\sqrt{x}) \\ &= 2x \sum_{d \leq \sqrt{x}} \frac{1}{d} - 2 \sum_{d \leq \sqrt{x}} d + O(\sqrt{x}) \\ &= 2x \left\{ \log \sqrt{x} + C + O\left(\frac{1}{\sqrt{x}}\right) \right\} - 2 \left\{ \frac{x}{2} + O(\sqrt{x}) \right\} + O(\sqrt{x}) \\ &= x \log x + (2C - 1)x + O(\sqrt{x}). \end{aligned}$$

Esto termina la demostración de la fórmula de Dirichlet. $\square$

Nota. El término de error $O(\sqrt{x})$ se puede mejorar. En 1903 Voronoi demostró que el error es $O(x^{1/3} \log x)$; en 1922 van de Corput lo mejoró hasta $O(x^{33/100})$. La mayor estimación hasta el presente es $O(x^{(12/37)+\varepsilon})$ para cada $\varepsilon > 0$, obtenida por Kolesnik [35] en 1969. La determinación del ínfimo de todos los θ tales que $O(x^\theta)$ sea el término de error constituye un problema abierto que se conoce con el nombre de problema del divisor de Dirichlet. En 1915 Hardy y Landau probaron que $\inf \theta \geq 1/4$.

3.6 EL ORDEN MEDIO DE LAS FUNCIONES DIVISOR $\sigma_\alpha(n)$

El caso $\alpha = 0$ se ha considerado en el teorema 3.3. Ahora consideramos $\alpha > 0$ real y tratamos el caso $\alpha = 1$ separadamente.

Teorema 3.4 Para todo $x \geq 1$ tenemos

$$(11) \quad \sum_{n \leq x} \sigma_1(n) = \frac{1}{2} \zeta(2) x^2 + O(x \log x).$$

Nota. Es posible demostrar que $\zeta(2) = \pi^2/6$. Por consiguiente (11) prueba que el orden medio de $\sigma_1(n)$ es $\pi^2 n/12$.

DEMOSTRACIÓN. El método es análogo al que se utilizó para obtener la versión más débil contenida en el teorema 3.3. Tenemos

$$\begin{aligned} \sum_{n \leq x} \sigma_1(n) &= \sum_{n \leq x} \sum_{q|n} q = \sum_{\substack{q, d \\ qd \leq x}} q = \sum_{d \leq x} \sum_{q \leq x/d} q \\ &= \sum_{d \leq x} \left\{ \frac{1}{2} \left(\frac{x}{d} \right)^2 + O\left(\frac{x}{d} \right) \right\} = \frac{x^2}{2} \sum_{d \leq x} \frac{1}{d^2} + O\left(x \sum_{d \leq x} \frac{1}{d} \right) \\ &= \frac{x^2}{2} \left\{ -\frac{1}{x} + \zeta(2) + O\left(\frac{1}{x^2} \right) \right\} + O(x \log x) = \frac{1}{2} \zeta(2) x^2 + O(x \log x), \end{aligned}$$

en donde hemos utilizado las partes (a) y (b) del teorema 3.2. $\square$

Teorema 3.5 Si $x \geq 1$ y $\alpha > 0$, $\alpha \neq 1$, tenemos

$$\sum_{n \leq x} \sigma_{\alpha}(n) = \frac{\zeta(\alpha + 1)}{\alpha + 1} x^{\alpha+1} + O(x^{\beta}),$$

en donde $\beta = \max \{1, \alpha\}$.

DEMOSTRACIÓN. Esta vez se utilizan las partes (b) y (d) del teorema 3.2 para obtener

$$\begin{aligned} \sum_{n \leq x} \sigma_{\alpha}(n) &= \sum_{n \leq x} \sum_{q|n} q^{\alpha} = \sum_{d \leq x} \sum_{q \leq x/d} q^{\alpha} \\ &= \sum_{d \leq x} \left\{ \frac{1}{\alpha + 1} \left(\frac{x}{d} \right)^{\alpha+1} + O\left(\frac{x^{\alpha}}{d^{\alpha}} \right) \right\} = \frac{x^{\alpha+1}}{\alpha + 1} \sum_{d \leq x} \frac{1}{d^{\alpha+1}} + O\left(x^{\alpha} \sum_{d \leq x} \frac{1}{d^{\alpha}} \right) \\ &= \frac{x^{\alpha+1}}{\alpha + 1} \left\{ \frac{x^{-\alpha}}{-\alpha} + \zeta(\alpha + 1) + O(x^{-\alpha-1}) \right\} \\ &\quad + O\left(x^{\alpha} \left\{ \frac{x^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O(x^{-\alpha}) \right\} \right) \\ &= \frac{\zeta(\alpha + 1)}{\alpha + 1} x^{\alpha+1} + O(x) + O(1) + O(x^{\alpha}) = \frac{\zeta(\alpha + 1)}{\alpha + 1} x^{\alpha+1} + O(x^{\beta}) \end{aligned}$$

en donde $\beta = \max \{1, \alpha\}$. □

Para buscar el orden medio de $\sigma_{\alpha}(n)$ para α negativo escribimos $\alpha = -\beta$, en donde $\beta > 0$.

Teorema 3.6. Si $\beta > 0$, sea $\delta = \max \{0, 1 - \beta\}$. Entonces, si $x > 1$, tenemos

$$\begin{aligned} \sum_{n \leq x} \sigma_{-\beta}(n) &= \zeta(\beta + 1)x + O(x^{\delta}) \quad \text{si } \beta \neq 1, \\ &= \zeta(2)x + O(\log x) \quad \text{si } \beta = 1. \end{aligned}$$

DEMOSTRACIÓN. Tenemos

$$\begin{aligned} \sum_{n \leq x} \sigma_{-\beta}(n) &= \sum_{n \leq x} \sum_{d|n} \frac{1}{d^{\beta}} = \sum_{d \leq x} \frac{1}{d^{\beta}} \sum_{q \leq x/d} 1 \\ &= \sum_{d \leq x} \frac{1}{d^{\beta}} \left\{ \frac{x}{d} + O(1) \right\} = x \sum_{d \leq x} \frac{1}{d^{\beta+1}} + O\left(\sum_{d \leq x} \frac{1}{d^{\beta}} \right). \end{aligned}$$

Este último término es $O(\log x)$ si $\beta = 1$ y $O(x^\delta)$ si $\beta \neq 1$. Puesto que

$$x \sum_{d \leq x} \frac{1}{d^{\beta+1}} = \frac{x^{1-\beta}}{-\beta} + \zeta(\beta+1)x + O(x^{-\beta}) = \zeta(\beta+1)x + O(x^{1-\beta})$$

esto termina la demostración. □

3.7 EL ORDEN MEDIO DE $\varphi(n)$

La fórmula asintótica relativa a las sumas parciales de la indicatriz de Euler contiene la suma de la serie

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}.$$

Esta serie converge absolutamente puesto que está dominada por $\sum_{n=1}^{\infty} n^{-2}$. En un capítulo posterior probaremos que

$$(12) \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Admitiendo de momento este resultado, tenemos

$$\begin{aligned} \sum_{n \leq x} \frac{\mu(n)}{n^2} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n > x} \frac{\mu(n)}{n^2} \\ &= \frac{6}{\pi^2} + O\left(\sum_{n > x} \frac{1}{n^2}\right) = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right) \end{aligned}$$

en virtud de la parte (c) del teorema 3.2. Utilizamos este resultado para obtener el orden medio de $\varphi(n)$.

Teorema 3.7 *Para $x > 1$ tenemos*

$$(13) \quad \sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \log x),$$

luego el orden medio de $\varphi(n)$ es $3n/\pi^2$.

DEMOSTRACIÓN. El método es análogo al utilizado para las funciones divisor. Empezamos con la relación

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

y obtenemos

$$\begin{aligned} \sum_{n \leq x} \varphi(n) &= \sum_{n \leq x} \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{\substack{q, d \\ qd \leq x}} \mu(d) q = \sum_{d \leq x} \mu(d) \sum_{q \leq x/d} q \\ &= \sum_{d \leq x} \mu(d) \left\{ \frac{1}{2} \left(\frac{x}{d} \right)^2 + O\left(\frac{x}{d} \right) \right\} \\ &= \frac{1}{2} x^2 \sum_{d \leq x} \frac{\mu(d)}{d^2} + O\left(x \sum_{d \leq x} \frac{1}{d} \right) \\ &= \frac{1}{2} x^2 \left\{ \frac{6}{\pi^2} + O\left(\frac{1}{x} \right) \right\} + O(x \log x) = \frac{3}{\pi^2} x^2 + O(x \log x). \quad \square \end{aligned}$$

3.8 UNA APLICACIÓN A LA DISTRIBUCIÓN DE LOS PUNTOS RETICULARES VISIBLES DESDE EL ORIGEN

La fórmula asintótica para las sumas parciales de $\varphi(n)$ tiene una interesante aplicación a un teorema concerniente a la distribución de puntos reticulares del plano que son visibles desde el origen.

Definición. Dos puntos reticulares P y Q se llaman mutuamente visibles si el segmento rectilíneo que los une no contiene otros puntos reticulares que los puntos extremos P y Q .

Teorema 3.8 *Dos puntos reticulares (a, b) y (m, n) son mutuamente visibles si, y sólo si, $a - m$ y $b - n$ son primos entre sí.*

DEMOSTRACIÓN. Es claro que (a, b) y (m, n) son mutuamente visibles si, y sólo si $(a - m, b - n)$, es visible desde el origen. Por lo tanto es suficiente probar el teorema cuando $(m, n) = (0, 0)$.

Suponemos que (a, b) es visible desde el origen, y hacemos $d = (a, b)$. Pretendemos demostrar que $d = 1$. Si $d > 1$, entonces $a = da'$, $b = db'$ y el punto reticular (a', b') se halla sobre el segmento rectilíneo que une $(0, 0)$ con (a, b) . Esta contradicción prueba que $d = 1$.

Recíprocamente, suponemos $(a, b) = 1$. Si un punto reticular (a', b') se halla en el segmento que une $(0, 0)$ con (a, b) tenemos

$$a' = ta, \quad b' = tb, \quad \text{en donde } 0 < t < 1.$$

Por lo tanto t es racional, luego $t = r/s$, en donde r, s son enteros positivos con $(r, s) = 1$. Luego

$$sa' = ar \quad \text{y} \quad sb' = br,$$

y por lo tanto $s|ar$, $s|br$. Pero $(s, r) = 1$, luego $s|a$, $s|b$. Por lo tanto $s = 1$ ya que $(a, b) = 1$. Esto contradice la desigualdad $0 < t < 1$. Por consiguiente el punto reticular (a, b) es visible desde el origen. $\square$

Existe una infinidad de puntos reticulares visibles desde el origen y es natural preguntarse cómo se hallan distribuidos en el plano.

Consideremos una región cuadrada amplia del plano xy definida por las desigualdades

$$|x| \leq r, \quad |y| \leq r.$$

Si $N(r)$ designa el número de puntos reticulares de este cuadrado, y si $N'(r)$ designa el número de los que son visibles desde el origen, el cociente $N'(r)/N(r)$ mide la fracción de puntos del cuadrado que son visibles desde el origen. El teorema que sigue prueba que esta fracción tiende a un límite cuando $r \rightarrow \infty$. Este límite se llama la *densidad* de los puntos reticulares visibles desde el origen.

Teorema 3.9 *El conjunto de puntos reticulares visibles desde el origen tiene densidad $6/\pi^2$.*

DEMOSTRACIÓN. Probaremos que

$$\lim_{r \rightarrow \infty} \frac{N'(r)}{N(r)} = \frac{6}{\pi^2}.$$

Los ocho puntos reticulares más próximos al origen son todos ellos visibles desde el origen (ver figura 3.3). Por simetría, vemos que $N'(r)$ es igual a 8, más 8 veces el número de puntos visibles de la región

$$\{(x, y): 2 \leq x \leq r, \quad 1 \leq y \leq x\},$$

(la región sombreada de la figura 3.3). Este número es

$$N'(r) = 8 + 8 \sum_{2 \leq n \leq r} \sum_{\substack{1 \leq m < n \\ (m, n) = 1}} 1 = 8 \sum_{1 \leq n \leq r} \varphi(n).$$

Utilizando el teorema 3.7 tenemos

$$N'(r) = \frac{24}{\pi^2} r^2 + O(r \log r).$$

Pero el número total de puntos reticulares del cuadrado es

$$N(r) = (2[r] + 1)^2 = (2r + O(1))^2 = 4r^2 + O(r)$$

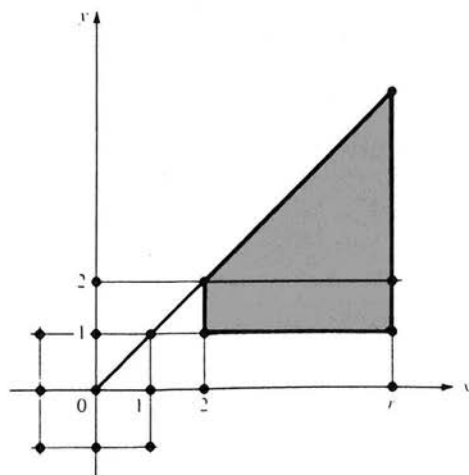


Figura 3.3

o sea

$$\frac{N'(r)}{N(r)} = \frac{\frac{24}{\pi^2} r^2 + O(r \log r)}{4r^2 + O(r)} = \frac{\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)}{1 + O\left(\frac{1}{r}\right)}.$$

Por lo tanto, cuando $r \rightarrow \infty$, obtenemos $N'(r)/N(r) \rightarrow 6/\pi^2$. □

Nota. El resultado del teorema 3.9 se describe algunas veces diciendo que un punto reticular elegido al azar tiene probabilidad $6/\pi^2$ de ser visible desde el origen. Luego, si dos enteros a y b se eligen al azar, la probabilidad de que sean primos entre sí es $6/\pi^2$.

3.9 EL ORDEN DE $\mu(n)$ Y EL DE $\Lambda(n)$

Los órdenes medios de $\mu(n)$ y $\Lambda(n)$ son considerablemente más difíciles de determinar que los de $\varphi(n)$ y que los de las funciones divisor. Es conocido que $\mu(n)$ tiene orden medio 0 y que $\Lambda(n)$ tiene orden medio 1. Esto es,

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \mu(n) = 0$$

y

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \Lambda(n) = 1,$$

pero las demostraciones no son simples. En el próximo capítulo probaremos que estos dos resultados son equivalentes al teorema del número primo,

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1,$$

en donde $\pi(x)$ es el número de primos $\leq x$.

En este capítulo obtenemos algunas identidades elementales que contienen a $\mu(n)$ y a $\Lambda(n)$ y que se utilizarán más adelante para estudiar la distribución de primos. Se deducirán de una fórmula general que relaciona las sumas parciales de funciones aritméticas arbitrarias f y g con su producto de Dirichlet $f * g$.

3.10 LAS SUMAS PARCIALES DE UN PRODUCTO DE DIRICHLET

Teorema 3.10 Si $h = f * g$, sea

$$H(x) = \sum_{n \leq x} h(n), \quad F(x) = \sum_{n \leq x} f(n), \quad \text{y} \quad G(x) = \sum_{n \leq x} g(n).$$

Entonces tenemos

$$(14) \quad H(x) = \sum_{n \leq x} f(n)G\left(\frac{x}{n}\right) = \sum_{n \leq x} g(n)F\left(\frac{x}{n}\right).$$

DEMOSTRACIÓN. Hacemos uso de la ley asociativa (teorema 2.21) que relaciona las operaciones $\circ$ y $*$. Sea

$$U(x) = \begin{cases} 0 & \text{si } 0 < x < 1, \\ 1 & \text{si } x \geq 1. \end{cases}$$

Entonces $F = f \circ U$, $G = g \circ U$, y tenemos

$$\begin{aligned} f \circ G &= f \circ (g \circ U) = (f * g) \circ U = H, \\ g \circ F &= g \circ (f \circ U) = (g * f) \circ U = H. \end{aligned}$$

Esto termina la demostración. □

Si $g(n) = 1$ para todo n entonces $G(x) = [x]$, y (14) nos proporciona el siguiente corolario:

Teorema 3.11 Si $F(x) = \sum_{n \leq x} f(n)$ tenemos

$$(15) \quad \sum_{n \leq x} \sum_{d|n} f(d) = \sum_{n \leq x} f(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} F\left(\frac{x}{n}\right).$$

3.11 APLICACIONES A $\mu(n)$ Y A $\Lambda(n)$

Ahora en el teorema 3.11 hacemos $f(n) = \mu(n)$ y $\Lambda(n)$ y obtenemos las identidades que siguen que utilizaremos más adelante para estudiar la distribución de primos.

Teorema 3.12 Para $x \geq 1$ tenemos

$$(16) \quad \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = 1$$

y

$$(17) \quad \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \log [x]!.$$

DEMOSTRACIÓN. De (15) obtenemos

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} \sum_{d|n} \mu(d) = \sum_{n \leq x} \left[\frac{1}{n} \right] = 1$$

y

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{n \leq x} \log n = \log [x]!. \quad \square$$

Nota. Las sumas que intervienen en el teorema 3.12 deben considerarse como medias ponderadas de las funciones $\mu(n)$ y $\Lambda(n)$.

En el teorema 4.16 demostraremos que el teorema del número primo se sigue de la afirmación que establece que la serie

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$$

converge y tiene suma 0. Utilizando (16) podemos demostrar que esta serie posee sumas parciales acotadas.

Teorema 3.13 Para todo $x \geq 1$ tenemos

$$(18) \quad \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1,$$

y la igualdad se verifica únicamente si $x < 2$.

DEMOSTRACIÓN. Si $x < 2$ sólo existe un término en la suma, $\mu(1) = 1$. Suponemos ahora que $x \geq 2$. Para cada real y , sea $\{y\} = y - [y]$. Entonces

$$1 = \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} \mu(n) \left(\frac{x}{n} - \left\{ \frac{x}{n} \right\} \right) = x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n) \left\{ \frac{x}{n} \right\}.$$

Puesto que $0 \leq \{y\} < 1$ esto implica

$$\begin{aligned} x \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| &= \left| 1 + \sum_{n \leq x} \mu(n) \left\{ \frac{x}{n} \right\} \right| \leq 1 + \sum_{n \leq x} \left\{ \frac{x}{n} \right\} \\ &= 1 + \{x\} + \sum_{2 \leq n \leq x} \left\{ \frac{x}{n} \right\} < 1 + \{x\} + [x] - 1 = x. \end{aligned}$$

Dividiendo por x obtenemos (18) con desigualdad estricta. □

Ahora volvemos a la identidad (17) del teorema 3.12,

$$(17) \quad \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \log[x]!,$$

y la utilizamos para determinar las potencias de números primos que dividen a una factorial.

Teorema 3.14 Identidad de Legendre. Para $x \geq 1$ tenemos

$$(19) \quad [x]! = \prod_{p \leq x} p^{\alpha(p)}$$

en donde el producto se halla extendido a todos los primos $\leq x$, y

$$(20) \quad \alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right].$$

Nota. La suma de $\alpha(p)$ es finita puesto que $[x/p^m] = 0$ para $p > x$.

DEMOSTRACIÓN. Puesto que $\Lambda(n) = 0$ a menos que n sea una potencia de primo, y $\Lambda(p^m) = \log p$, tenemos

$$\log[x]! = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \sum_{p \leq x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right] \log p = \sum_{p \leq x} \alpha(p) \log p,$$

en donde $\alpha(p)$ está dado por (20). La última suma es el logaritmo del producto de (19), lo que termina la demostración. $\square$

Ahora utilizaremos la fórmula de sumación de Euler para determinar una fórmula asintótica para $\log[x]!$

Teorema 3.15 Si $x \geq 2$ tenemos

$$(21) \quad \log[x]! = x \log x - x + O(\log x),$$

y por lo tanto

$$(22) \quad \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = x \log x - x + O(\log x).$$

DEMOSTRACIÓN. Si hacemos $f(t) = \log t$ en la fórmula de sumación de Euler (teorema 3.1), obtenemos

$$\begin{aligned} \sum_{n \leq x} \log n &= \int_1^x \log t \, dt + \int_1^x \frac{t - [t]}{t} \, dt - (x - [x]) \log x \\ &= x \log x - x + 1 + \int_1^x \frac{t - [t]}{t} \, dt + O(\log x). \end{aligned}$$

Esto prueba (21) ya que

$$\int_1^x \frac{t - [t]}{t} \, dt = O\left(\int_1^x \frac{1}{t} \, dt\right) = O(\log x),$$

y (22) procede de (17).

El teorema que sigue es una consecuencia de (22).

Teorema 3.16 Para $x \geq 2$ tenemos

$$(23) \quad \sum_{p \leq x} \left[\frac{x}{p} \right] \log p = x \log x + O(x),$$

en donde la suma se halla extendida a todos los primos $\leq x$.

DEMOSTRACIÓN. Puesto que $\Lambda(n) = 0$ excepto si n es una potencia de primo, tenemos

$$\sum_{n \leq x} \left[\frac{x}{n} \right] \Lambda(n) = \sum_p \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \left[\frac{x}{p^m} \right] \Lambda(p^m).$$

Pero $p^m \leq x$ implica $p \leq x$. Además, $[x/p^m] = 0$ si $p > x$ por lo tanto podemos escribir la última suma en la forma

$$\sum_{p \leq x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right] \log p = \sum_{p \leq x} \left[\frac{x}{p} \right] \log p + \sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m} \right] \log p.$$

Ahora veremos que esta última suma es $O(x)$. Tenemos

$$\begin{aligned} \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \left[\frac{x}{p^m} \right] &\leq \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \frac{x}{p^m} = x \sum_{p \leq x} \log p \sum_{m=2}^{\infty} \left(\frac{1}{p} \right)^m \\ &= x \sum_{p \leq x} \log p \cdot \frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = x \sum_{p \leq x} \frac{\log p}{p(p-1)} \\ &\leq x \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(x). \end{aligned}$$

Por lo tanto hemos probado

$$\sum_{n \leq x} \left[\frac{x}{n} \right] \Lambda(n) = \sum_{p \leq x} \left[\frac{x}{p} \right] \log p + O(x),$$

que, usado junto con (22), prueba (23). $\square$

La ecuación (23) se utilizará en el capítulo siguiente para obtener una fórmula asintótica para las sumas parciales de la serie divergente $\sum (1/p)$.

3.12 OTRA IDENTIDAD PARA LAS SUMAS PARCIALES DE UN PRODUCTO DE DIRICHLET

Terminamos este capítulo con una versión más general del teorema 3.10 que utilizaremos en el capítulo 4 para estudiar las sumas parciales de ciertos productos de Dirichlet.

Como en el teorema 3.10 escribimos

$$F(x) = \sum_{n \leq x} f(n), \quad G(x) = \sum_{n \leq x} g(n), \quad \text{y} \quad H(x) = \sum_{n \leq x} (f * g)(n)$$

y entonces

$$H(x) = \sum_{n \leq x} \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{q, d \\ qd \leq x}} f(d)g(q).$$

Teorema 3.17 Si a y b son números reales positivos tales que $ab = x$, entonces

$$(24) \quad \sum_{\substack{q, d \\ qd \leq x}} f(d)g(q) = \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b).$$

DEMOSTRACIÓN. La suma $H(x)$ de la izquierda de (24) se halla extendida a todos los puntos reticulares de la región hiperbólica dibujada en la figura 3.4. Separamos la suma en dos partes, una extendida a los puntos reticulares de $A \cup B$ y la otra a los de $B \cup C$. Los puntos reticulares de B intervienen dos veces, por lo que tenemos

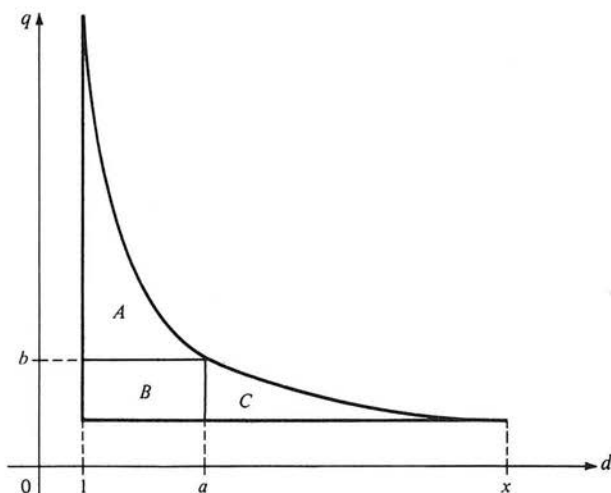


Figura 3.4

$$H(x) = \sum_{d \leq a} \sum_{q \leq x/d} f(d)g(q) + \sum_{q \leq b} \sum_{d \leq x/q} f(d)g(q) - \sum_{d \leq a} \sum_{q \leq b} f(d)g(q),$$

que es la misma que (24). □

Nota. Si tomamos $a = 1$ y $b = 1$, respectivamente, obtenemos las dos ecuaciones del teorema 3.10, puesto que $f(1) = F(1)$ y $g(1) = G(1)$.

Ejercicios del capítulo 3

1. Utilizar la fórmula de sumación de Euler para deducir las siguientes para $x \geq 2$:

(a) $\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + A + O\left(\frac{\log x}{x}\right)$, en donde A es constante.

(b) $\sum_{2 \leq n \leq x} \frac{1}{n \log n} = \log(\log x) + B + O\left(\frac{1}{x \log x}\right)$, en donde B es constante.

2. Si $x \geq 2$ probar que

$$\sum_{n \leq x} \frac{d(n)}{n} = \frac{1}{2} \log^2 x + 2C \log x + O(1), \text{ en donde } C \text{ es la constante de Euler.}$$

3. Si $x \geq 2$ y $\alpha > 0$, $\alpha \neq 1$, probar que

$$\sum_{n \leq x} \frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha} \log x}{1-\alpha} + \zeta(\alpha)^2 + O(x^{1-\alpha}).$$

4. Si $x \geq 2$ probar que:

$$(a) \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right]^2 = \frac{x^2}{\zeta(2)} + O(x \log x).$$

$$(b) \sum_{n \leq x} \frac{\mu(n)}{n} \left[\frac{x}{n} \right] = \frac{x}{\zeta(2)} + O(\log x).$$

5. Si $x \geq 1$ probar que:

$$(a) \sum_{n \leq x} \varphi(n) = \frac{1}{2} \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right]^2 + \frac{1}{2}.$$

$$(b) \sum_{n \leq x} \frac{\varphi(n)}{n} = \sum_{n \leq x} \frac{\mu(n)}{n} \left[\frac{x}{n} \right].$$

Estas fórmulas junto con las del ejercicio 4 prueban que, para $x \geq 2$,

$$\sum_{n \leq x} \varphi(n) = \frac{1}{2} \frac{x^2}{\zeta(2)} + O(x \log x) \quad \text{y} \quad \sum_{n \leq x} \frac{\varphi(n)}{n} = \frac{x}{\zeta(2)} + O(\log x).$$

6. Si $x \geq 2$ probar que

$$\sum_{n \leq x} \frac{\varphi(n)}{n^2} = \frac{1}{\zeta(2)} \log x + \frac{C}{\zeta(2)} - A + O\left(\frac{\log x}{x}\right),$$

en donde C es la constante de Euler y

$$A = \sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n^2}.$$

7. En un capítulo posterior demostraremos que $\sum_{n=1}^{\infty} \mu(n) n^{-\alpha} = 1/\zeta(\alpha)$ si $\alpha > 1$. Admitiendo este resultado, probar que para $x \geq 2$ y $\alpha > 1$, $\alpha \neq 2$, tenemos

$$\sum_{n \leq x} \frac{\varphi(n)}{n^\alpha} = \frac{x^{2-\alpha}}{2-\alpha} \frac{1}{\zeta(2)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O(x^{1-\alpha} \log x).$$

8. Si $\alpha \leq 1$ y $x \geq 2$ probar que

$$\sum_{n \leq x} \frac{\varphi(n)}{n^{\alpha}} = \frac{x^{2-\alpha}}{2-\alpha} \frac{1}{\zeta(2)} + O(x^{1-\alpha} \log x).$$

9. En un capítulo posterior probaremos que el producto infinito $\prod_p (1 - p^{-2})$, extendido a todos los primos, converge hacia el valor $1/\zeta(2) = 6/\pi^2$. Admitiendo este resultado, probar que

$$(a) \quad \frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n} \quad \text{si } n \geq 2.$$

[Indicación: Usar la fórmula $\varphi(n) = n \prod_{p|n} (1 - p^{-1})$ y la relación

$$1 + x + x^2 + \cdots = \frac{1}{1-x} = \frac{1+x}{1-x^2} \quad \text{con } x = \frac{1}{p}.]$$

- (b) Si $x \geq 2$ probar que

$$\sum_{n \leq x} \frac{n}{\varphi(n)} = O(x).$$

10. Si $x \geq 2$ probar que

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = O(\log x).$$

11. Sea $\varphi_1(n) = n \sum_{d|n} \mu(d)/d$.

- (a) Probar que φ_1 es multiplicativa y que $\varphi_1(n) = n \prod_{p|n} (1 + p^{-1})$.
(b) Probar que

$$\varphi_1(n) = \sum_{d^2|n} \mu(d) \sigma\left(\frac{n}{d^2}\right)$$

en donde la suma se halla extendida a los divisores de n tales que $d^2|n$.

- (c) Probar que

$$\sum_{n \leq x} \varphi_1(n) = \sum_{d \leq \sqrt{x}} \mu(d) S\left(\frac{x}{d^2}\right), \quad \text{en donde } S(x) = \sum_{k \leq x} \sigma(k),$$

y entonces utilizar el teorema 3.4 para deducir que, para $x \geq 2$,

$$\sum_{n \leq x} \varphi_1(n) = \frac{\zeta(2)}{2\zeta(4)} x^2 + O(x \log x).$$

Igual que en el ejercicio 7, podemos suponer válido el resultado $\sum_{n=1}^{\infty} \mu(n) n^{-\alpha} = 1/\zeta(\alpha)$ para $\alpha > 1$.

12. Para s real > 0 y para k entero ≥ 1 hallar una fórmula asintótica para la suma parcial

$$\sum_{\substack{n \leq x \\ (n, k) = 1}} \frac{1}{n^s}.$$

con un término de error que tienda a 0 cuando $x \rightarrow \infty$. Asegurarse de que el caso $s = 1$ se halla incluido.

PROPIEDADES DE LA FUNCIÓN PARTE ENTERA

Para cada real x el símbolo $[x]$ designa el mayor entero $\leq x$. Los ejercicios 13 al 26 describen algunas propiedades de la función parte entera. En estos ejercicios x e y designan números reales, n designa un entero.

13. Probar cada una de las afirmaciones siguientes:

(a) Si $x = k + y$ en donde k es un entero y $0 \leq y < 1$, entonces $k = [x]$.

(b) $[x + n] = [x] + n$.

(c) $[-x] = \begin{cases} -[x] & \text{si } x = [x], \\ -[x] - 1 & \text{si } x \neq [x]. \end{cases}$

(d) $[x/n] = [[x]/n]$ si $n \geq 1$.

14. Si $0 < y < 1$, ¿cuáles son los valores posibles de $[x] - [x - y]$?

15. El número $\{x\} = x - [x]$ se llama *parte residual* de x . Satisface las desigualdades $0 \leq \{x\} < 1$, con $\{x\} = 0$ si, y sólo si, x es un entero. ¿Cuáles son los valores posibles de $\{x\} + \{-x\}$?

16. (a) Probar que $[2x] - 2[x]$ es 0 o 1.

(b) Probar que $[2x] + [2y] \geq [x] + [y] + [x + y]$.

17. Probar que $[x] + [x + \frac{1}{2}] = [2x]$ y, en general,

$$\sum_{k=0}^{n-1} \left[x + \frac{k}{n} \right] = [nx].$$

18. Sea $f(x) = x - [x] - \frac{1}{2}$. Probar que

$$\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx)$$

y deducir que

$$\left| \sum_{n=1}^m f\left(2^n x + \frac{1}{2}\right) \right| \leq 1 \quad \text{para todo } m \geq 1 \text{ y todo real } x.$$

19. Dados dos enteros positivos impares h y k , con $(h, k) = 1$, sean $a = (k-1)/2$, $b = (h-1)/2$.

(a) Probar que $\sum_{r=1}^a [hr/k] + \sum_{r=1}^b [kr/h] = ab$. *Indicación.* Puntos reticulares.

(b) Obtener el resultado correspondiente si $(h, k) = d$.

20. Si n es un entero positivo probar que $[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}]$.

21. Determinar todos los enteros positivos n tales que $[\sqrt{n}]$ divide a n .

22. Si n es un entero positivo, probar que

$$\left[\frac{8n+13}{25} \right] - \left[\frac{n-12 - \left[\frac{n-17}{25} \right]}{3} \right]$$

es independiente de n .

23. Probar que

$$\sum_{n \leq x} \lambda(n) \left[\frac{x}{n} \right] = [\sqrt{x}].$$

24. Probar que

$$\sum_{n \leq x} \left[\sqrt{\frac{x}{n}} \right] = \sum_{n \leq \sqrt{x}} \left[\frac{x}{n^2} \right].$$

25. Probar que

$$\sum_{k=1}^n \left[\frac{k}{2} \right] = \left[\frac{n^2}{4} \right]$$

y que

$$\sum_{k=1}^n \left[\frac{k}{3} \right] = \left[\frac{n(n-1)}{6} \right].$$

26. Si $a = 1, 2, \dots, 7$ probar que existe un entero b (dependiente de a) tal que

$$\sum_{k=1}^n \left[\frac{k}{a} \right] = \left[\frac{(2n+b)^2}{8a} \right].$$

Capítulo 4

Algunos teoremas elementales sobre la distribución de los números primos

4.1 INTRODUCCIÓN

Si $x > 0$, $\pi(x)$ designa el número de primos que no exceden a x . Entonces $\pi(x) \rightarrow \infty$ cuando $x \rightarrow \infty$ puesto que existe una infinidad de números primos. El comportamiento de $\pi(x)$ como función de x ha sido objeto de un intenso estudio por parte de muchos matemáticos ilustres a partir del siglo dieciocho. La inspección de tablas de primos condujeron a Gauss (1792) y Legendre (1798) a conjeturar que $\pi(x)$ es asintótica a $x/\log x$, es decir,

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

Tal conjetura fue demostrada en 1896 por Hadamard [28] y por de la Vallée Poussin [71] y se conoce con el nombre de *teorema del número primo*.

Las demostraciones del teorema del número primo se clasifican a menudo en *analíticas* y *elementales*, según los métodos utilizados para desarrollarlas. La demostración de Hadamard y de la Vallée Poussin es analítica, utilizando la teoría de las funciones de variable compleja y propiedades de la función zeta de Riemann. Una demostración elemental fue hallada en 1949 por A. Selberg y P. Erdős. Su demostración no recurre a la función zeta ni a la teoría de las funciones complejas pero es bastante intrincada. Al final de este capítulo damos un breve esbozo de

los puntos más destacados de la demostración elemental. En el capítulo 13 daremos una demostración analítica breve que es más transparente que la demostración elemental.

Este capítulo trata primordialmente de teoremas elementales acerca de los números primos. En particular, probaremos que el teorema del número primo se puede expresar de varias formas equivalentes.

Por ejemplo, probaremos que el teorema del número primo es equivalente a la fórmula asintótica

$$(1) \quad \sum_{n \leq x} \Lambda(n) \sim x \quad \text{cuando } x \rightarrow \infty.$$

Las sumas parciales de la función de Mangoldt $\Lambda(n)$ definen una función introducida por Chebyshev en 1848.

4.2 LAS FUNCIONES DE CHEBYSHEV $\psi(x)$ Y $\vartheta(x)$

Definición. Para cada $x > 0$ definimos la función ψ de Chebyshev por la fórmula

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Entonces, la fórmula asintótica dada en (1) establece que

$$(2) \quad \lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1.$$

Puesto que $\Lambda(n) = 0$ excepto si n es una potencia de primo podemos escribir la definición de $\psi(x)$ como sigue:

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \sum_p \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p.$$

La suma extendida a m es, en realidad, una suma finita. De hecho, la suma extendida a p es vacía si $x^{1/m} < 2$, es decir, si $(1/m) \log x < \log 2$, o si

$$m > \frac{\log x}{\log 2} = \log_2 x.$$

Por consiguiente tenemos

$$\psi(x) = \sum_{m \leq \log_2 x} \sum_{p \leq x^{1/m}} \log p.$$

Esto puede escribirse de forma ligeramente diferente introduciendo otra función de Chebyshev.

Definición. Si $x > 0$ definimos la función ϑ de Chebyshev por la ecuación

$$\vartheta(x) = \sum_{p \leq x} \log p,$$

en donde p recorre todos los primos $\leq x$.

La última fórmula dada para $\psi(x)$ se puede escribir ahora como sigue:

$$(3) \quad \psi(x) = \sum_{m \leq \log_2 x} \vartheta(x^{1/m}).$$

El teorema siguiente relaciona los dos cocientes $\psi(x)/x$ y $\vartheta(x)/x$.

Teorema 4.1 Para $x > 0$ tenemos

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x} \log 2}.$$

Nota. Esta desigualdad implica

$$\lim_{x \rightarrow \infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0.$$

Con otras palabras, si uno de los cocientes $\psi(x)/x$ o $\vartheta(x)/x$ posee límite entonces el otro cociente también y ambos límites coinciden.

DEMOSTRACIÓN. De (3) obtenemos

$$0 \leq \psi(x) - \vartheta(x) = \sum_{2 \leq m \leq \log_2 x} \vartheta(x^{1/m}).$$

Pero de la definición de $\vartheta(x)$ obtenemos la desigualdad trivial

$$\vartheta(x) \leq \sum_{p \leq x} \log x \leq x \log x$$

luego

$$\begin{aligned} 0 \leq \psi(x) - \vartheta(x) &\leq \sum_{2 \leq m \leq \log_2 x} x^{1/m} \log(x^{1/m}) \leq (\log_2 x) \sqrt{x} \log \sqrt{x} \\ &= \frac{\log x}{\log 2} \cdot \frac{\sqrt{x}}{2} \log x = \frac{\sqrt{x} (\log x)^2}{2 \log 2}. \end{aligned}$$

Dividimos ahora por x y obtenemos el teorema. □

4.3 RELACIONES QUE LIGAN $\vartheta(x)$ Y $\pi(x)$

En esta sección obtenemos dos fórmulas que relacionan $\vartheta(x)$ y $\pi(x)$. Se utilizarán para demostrar que el teorema del número primo es equivalente a la relación límite

$$\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1.$$

Las dos funciones $\pi(x)$ y $\vartheta(x)$ son funciones escalonadas con salto en los números primos; $\pi(x)$ tiene salto 1 en cada primo p , mientras que $\vartheta(x)$ tiene salto $\log p$ en p . Las sumas que contienen funciones escalonadas de este tipo se pueden expresar como integrales por medio del teorema que sigue.

Teorema 4.2 Identidad de Abel. *Para toda función aritmética $a(n)$, sea*

$$A(x) = \sum_{n \leq x} a(n),$$

en donde $A(x) = 0$ si $x < 1$. Suponemos que f posee derivada continua en el intervalo $[y, x]$, en donde $0 < y < x$. Entonces tenemos

$$(4) \quad \sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t) dt.$$

DEMOSTRACIÓN. Sea $k = [x]$ y $m = [y]$, por lo que $A(x) = A(k)$ y $A(y) = A(m)$. Entonces

$$\begin{aligned}
 \sum_{y < n \leq x} a(n)f(n) &= \sum_{n=m+1}^k a(n)f(n) = \sum_{n=m+1}^k \{A(n) - A(n-1)\}f(n) \\
 &= \sum_{n=m+1}^k A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\
 &= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1) \\
 &= - \sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t) dt + A(k)f(k) - A(m)f(m+1) \\
 &= - \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t) dt + A(k)f(k) - A(m)f(m+1) \\
 &= - \int_{m+1}^k A(t)f'(t) dt + A(x)f(x) - \int_k^x A(t)f'(t) dt \\
 &\quad - A(y)f(y) - \int_y^{m+1} A(t)f'(t) dt \\
 &= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t) dt.
 \end{aligned}$$

□

OTRA DEMOSTRACIÓN. Una demostración breve de (4) se puede dar para aquellos lectores familiarizados con la integración de Riemann-Stieltjes. (Ver [2], capítulo 7.) Puesto que $A(x)$ es una función escalonada con salto $f(n)$ en cada entero n , la suma que interviene en (4) se puede expresar como una integral de Riemann-Stieltjes,

$$\sum_{y < n \leq x} a(n)f(n) = \int_y^x f(t) dA(t).$$

La integración por partes nos proporciona

$$\begin{aligned}
 \sum_{y < n \leq x} a(n)f(n) &= f(x)A(x) - f(y)A(y) - \int_y^x A(t) df(t) \\
 &= f(x)A(x) - f(y)A(y) - \int_y^x A(t)f'(t) dt.
 \end{aligned}$$

□

Nota. Puesto que $A(t) = 0$ si $t < 1$, cuando $y < 1$ la ecuación (4) toma la forma

$$(5) \quad \sum_{n \leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t) dt.$$

Observemos además que la fórmula de sumación de Euler se puede deducir fácilmente de (4). En efecto, si $a(n) = 1$ para todo $n \geq 1$ obtenemos $A(x) = [x]$ y (4) implica

$$\sum_{y < n \leq x} f(n) = f(x)[x] - f(y)[y] - \int_y^x [t]f'(t) dt.$$

Combinando esto con la fórmula de integración por partes

$$\int_y^x tf'(t) dt = xf(x) - yf(y) - \int_y^x f(t) dt$$

obtenemos inmediatamente la fórmula de sumación de Euler (teorema 3.1).

Ahora utilizamos (4) para expresar $\vartheta(x)$ y $\pi(x)$ por medio de integrales.

Teorema 4.3 Para $x \geq 2$ tenemos

$$(6) \quad \vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t} dt$$

y

$$(7) \quad \pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt.$$

DEMOSTRACIÓN. $a(n)$ designa la función característica de los primos; es decir

$$a(n) = \begin{cases} 1 & \text{si } n \text{ es primo,} \\ 0 & \text{en otro caso.} \end{cases}$$

Entonces tenemos

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{1 < n \leq x} a(n) \quad \text{y} \quad \vartheta(x) = \sum_{p \leq x} \log p = \sum_{1 < n \leq x} a(n)\log n.$$

Si hacemos $f(x) = \log x$ en (4) con $y = 1$ obtenemos

$$\vartheta(x) = \sum_{1 < n \leq x} a(n) \log n = \pi(x) \log x - \pi(1) \log 1 - \int_1^x \frac{\pi(t)}{t} dt,$$

que prueba (6) ya que $\pi(t) = 0$ para $t < 2$.

Ahora, sea $b(n) = a(n) \log n$ y escribamos

$$\pi(x) = \sum_{3/2 < n \leq x} b(n) \frac{1}{\log n}, \quad \vartheta(x) = \sum_{n \leq x} b(n).$$

Si hacemos $f(x) = 1/\log x$ en (4) con $y = 3/2$ obtenemos

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\vartheta(t)}{t \log^2 t} dt,$$

que prueba (7) ya que $\vartheta(t) = 0$ si $t < 2$. □

4.4 CIERTAS FORMAS EQUIVALENTES DEL TEOREMA DEL NÚMERO PRIMO

Teorema 4.4 *Las relaciones que siguen son lógicamente equivalentes:*

$$(8) \quad \lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

$$(9) \quad \lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = 1.$$

$$(10) \quad \lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1.$$

DEMOSTRACIÓN. De (6) y (7) obtenemos, respectivamente,

$$\frac{\vartheta(x)}{x} = \frac{\pi(x) \log x}{x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt$$

y

$$\frac{\pi(x) \log x}{x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt.$$

Para probar que (8) implica (9) únicamente necesitamos demostrar que (8) implica

$$\lim_{x \rightarrow \infty} \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = 0.$$

Pero (8) implica $\frac{\pi(t)}{t} = O\left(\frac{1}{\log t}\right)$ para $t \geq 2$ o sea

$$\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = O\left(\frac{1}{x} \int_2^x \frac{dt}{\log t}\right).$$

Ahora bien

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x - \sqrt{x}}{\log \sqrt{x}}$$

luego

$$\frac{1}{x} \int_2^x \frac{dt}{\log t} \rightarrow 0 \quad \text{cuando } x \rightarrow \infty.$$

Esto demuestra que (8) implica (9).

Para probar que (9) implica (8) únicamente necesitamos probar que (9) implica

$$\lim_{x \rightarrow \infty} \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt = 0.$$

Pero (9) implica $\vartheta(t) = O(t)$ luego

$$\frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt = O\left(\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t}\right).$$

Ahora bien

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x - \sqrt{x}}{\log^2 \sqrt{x}}$$

por lo tanto

$$\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} \rightarrow 0 \quad \text{cuando } x \rightarrow \infty.$$

Esto demuestra que (9) implica (8), luego (8) y (9) son equivalentes. En virtud del teorema 4.1 sabemos que (9) y (10) son equivalentes. $\square$

El teorema que sigue relaciona el teorema del número primo con el valor asintótico del n -ésimo número primo.

Teorema 4.5 Si p_n designa el primo n -ésimo, entonces las siguientes relaciones asintóticas son lógicamente equivalentes:

$$(11) \quad \lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

$$(12) \quad \lim_{x \rightarrow \infty} \frac{\pi(x) \log \pi(x)}{x} = 1.$$

$$(13) \quad \lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1.$$

DEMOSTRACIÓN. Probaremos que (11) implica (12), que (12) implica (13), que (13) implica (12), y que (12) implica (11).

Suponemos que se verifica (11). Tomando logaritmos obtenemos

$$\lim_{x \rightarrow \infty} [\log \pi(x) + \log \log x - \log x] = 0$$

luego

$$\lim_{x \rightarrow \infty} \left[\log x \left(\frac{\log \pi(x)}{\log x} + \frac{\log \log x}{\log x} - 1 \right) \right] = 0.$$

Puesto que $\log x \rightarrow \infty$ cuando $x \rightarrow \infty$ vemos que

$$\lim_{x \rightarrow \infty} \left(\frac{\log \pi(x)}{\log x} + \frac{\log \log x}{\log x} - 1 \right) = 0$$

de donde obtenemos

$$\lim_{x \rightarrow \infty} \frac{\log \pi(x)}{\log x} = 1.$$

Esto, junto con (11), nos da (12).

Ahora suponemos que se verifica (12). Si $x = p_n$ entonces $\pi(x) = n$ y

$$\pi(x) \log \pi(x) = n \log n$$

luego (12) implica

$$\lim_{n \rightarrow \infty} \frac{n \log n}{p_n} = 1.$$

Entonces (12) implica (13).

Ahora suponemos que se verifica (13). Dado x , definimos n por medio de las desigualdades

$$p_n \leq x < p_{n+1},$$

o sea que $n = \pi(x)$. Si dividimos por $n \log n$, obtenemos

$$\frac{p_n}{n \log n} \leq \frac{x}{n \log n} < \frac{p_{n+1}}{n \log n} = \frac{p_{n+1}}{(n+1) \log(n+1)} \frac{(n+1) \log(n+1)}{n \log n}.$$

Ahora suponemos que $n \rightarrow \infty$ y utilizamos (13) a fin de obtener

$$\lim_{n \rightarrow \infty} \frac{x}{n \log n} = 1, \text{ o bien } \lim_{x \rightarrow \infty} \frac{x}{\pi(x) \log \pi(x)} = 1.$$

Por consiguiente, (13) implica (12).

Finalmente, probaremos que (12) implica (11). Si tomamos logaritmos en (12) obtenemos

$$\lim_{x \rightarrow \infty} (\log \pi(x) + \log \log \pi(x) - \log x) = 0$$

o bien

$$\lim_{x \rightarrow \infty} \left[\log \pi(x) \left(1 + \frac{\log \log \pi(x)}{\log \pi(x)} - \frac{\log x}{\log \pi(x)} \right) \right] = 0.$$

Puesto que $\log \pi(x) \rightarrow \infty$ se tiene que

$$\lim_{x \rightarrow \infty} \left(1 + \frac{\log \log \pi(x)}{\log \pi(x)} - \frac{\log x}{\log \pi(x)} \right) = 0$$

luego

$$\lim_{x \rightarrow \infty} \frac{\log x}{\log \pi(x)} = 1.$$

Esto, junto con (12), nos da (11). □

4.5 DESIGUALDADES RELATIVAS A $\pi(n)$ Y A p_n

El teorema del número primo establece que $\pi(n) \sim n/\log n$ cuando $n \rightarrow \infty$. Las desigualdades del próximo teorema prueban que $n/\log n$ es el orden de magnitud correcto de $\pi(n)$. Aunque con un mayor esfuerzo es posible mejorar las desigualdades (ver [60]), el teorema que sigue es interesante por la naturaleza elemental de su demostración.

Teorema 4.6 *Para cada entero $n \geq 2$ tenemos*

$$(14) \quad \frac{1}{6} \frac{n}{\log n} < \pi(n) < 6 \frac{n}{\log n}.$$

DEMOSTRACIÓN. Empezamos con las desigualdades

$$(15) \quad 2^n \leq \binom{2n}{n} < 4^n,$$

en donde $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ es un número combinatorio. La desigualdad de más a la derecha se sigue de la relación

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n},$$

y la otra es fácil demostrarla por inducción. Tomando logaritmos en (15) obtenemos

$$(16) \quad n \log 2 \leq \log(2n)! - 2 \log n! < n \log 4.$$

Pero el teorema 3.14 implica

$$\log n! = \sum_{p \leq n} \alpha(p) \log p$$

en donde la suma se halla extendida a todos los primos y $\alpha(p)$ es

$$\alpha(p) = \sum_{m=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^m} \right\rfloor.$$

Por lo tanto

$$(17) \quad \log(2n)! - 2 \log n! = \sum_{p \leq 2n} \sum_{m=1}^{\left\lfloor \frac{\log 2n}{\log p} \right\rfloor} \left\{ \left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right\} \log p.$$

Puesto que $[2x] - 2[x]$ es 0 o 1, el primer miembro de la desigualdad (16) implica

$$n \log 2 \leq \sum_{p \leq 2n} \left(\sum_{m=1}^{\left\lfloor \frac{\log 2n}{\log p} \right\rfloor} 1 \right) \log p \leq \sum_{p \leq 2n} \log 2n = \pi(2n) \log 2n.$$

Esto nos da

$$(18) \quad \pi(2n) \geq \frac{n \log 2}{\log 2n} = \frac{2n}{\log 2n} \frac{\log 2}{2} > \frac{1}{4} \frac{2n}{\log 2n}$$

puesto que $\log 2 > 1/2$. Para los enteros impares tenemos

$$\pi(2n+1) \geq \pi(2n) > \frac{1}{4} \frac{2n}{\log 2n} > \frac{1}{4} \frac{2n}{2n+1} \frac{2n+1}{\log(2n+1)} \geq \frac{1}{6} \frac{2n+1}{\log(2n+1)}$$

puesto que $2n/(2n+1) \geq 2/3$. Esto, junto con (18), nos da

$$\pi(n) > \frac{1}{6} \frac{n}{\log n}$$

para todo $n \geq 2$, que prueba la primera desigualdad de (14).

Para demostrar la otra desigualdad volvemos a (17) y extraemos los términos que corresponden a $m=1$. Los términos restantes son no negativos por lo que tenemos

$$\log(2n)! - 2 \log n! \geq \sum_{p \leq 2n} \left\{ \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] \right\} \log p.$$

Para los primos p del intervalo $n < p \leq 2n$ tenemos $[2n/p] - 2[n/p] = 1$, o sea

$$\log(2n)! - 2 \log n! \geq \sum_{n < p \leq 2n} \log p = \vartheta(2n) - \vartheta(n).$$

Por lo tanto, (16) implica

$$\vartheta(2n) - \vartheta(n) < n \log 4.$$

En particular, si n es una potencia de 2, obtenemos

$$\vartheta(2^{r+1}) - \vartheta(2^r) < 2^r \log 4 = 2^{r+1} \log 2.$$

Si sumamos para $r = 0, 1, 2, \dots, k$, la suma del primer miembro se reduce, obteniéndose

$$\vartheta(2^{k+1}) < 2^{k+2} \log 2.$$

Ahora elegimos k de forma que $2^k \leq n < 2^{k+1}$ y obtenemos

$$\vartheta(n) \leq \vartheta(2^{k+1}) < 2^{k+2} \log 2 \leq 4n \log 2.$$

Pero, si $0 < \alpha < 1$, tenemos

$$(\pi(n) - \pi(n^\alpha)) \log n^\alpha < \sum_{n^\alpha < p \leq n} \log p \leq \vartheta(n) < 4n \log 2,$$

por lo tanto

$$\begin{aligned} \pi(n) &< \frac{4n \log 2}{\alpha \log n} + \pi(n^\alpha) < \frac{4n \log 2}{\alpha \log n} + n^\alpha \\ &= \frac{n}{\log n} \left(\frac{4 \log 2}{\alpha} + \frac{\log n}{n^{1-\alpha}} \right). \end{aligned}$$

Ahora, si $c > 0$ y $x \geq 1$, la función $f(x) = x^{-c} \log x$ alcanza su máximo en $x = e^{1/c}$, o sea que $n^{-c} \log n \leq 1/(ce)$ para $n \geq 1$. Si tomamos $\alpha = 2/3$ en la última desigualdad relativa a $\pi(n)$ obtenemos

$$\pi(n) < \frac{n}{\log n} \left(6 \log 2 + \frac{3}{e} \right) < 6 \frac{n}{\log n}.$$

Esto termina la demostración. □

El teorema 4.6 sirve para obtener cotas superiores e inferiores del tamaño del n -ésimo número primo.

Teorema 4.7 Para $n \geq 1$ el n -ésimo primo p_n satisface las desigualdades

$$(19) \quad \frac{1}{6} n \log n < p_n < 12 \left(n \log n + n \log \frac{12}{e} \right).$$

DEMOSTRACIÓN. Si $k = p_n$ entonces $k \geq 2$ y $n = \pi(k)$. De (14) obtenemos

$$n = \pi(k) < 6 \frac{k}{\log k} = 6 \frac{p_n}{\log p_n}$$

luego

$$p_n > \frac{1}{6} n \log p_n > \frac{1}{6} n \log n.$$

Esto nos proporciona la cota inferior de (19).

Para obtener la cota superior utilizamos nuevamente (14) para escribir

$$n = \pi(k) > \frac{1}{6} \frac{k}{\log k} = \frac{1}{6} \frac{p_n}{\log p_n},$$

de donde se obtiene

$$(20) \quad p_n < 6n \log p_n.$$

Puesto que $\log x \leq (2/e) \sqrt{x}$ si $x \geq 1$ tenemos $\log p_n \leq (2/e) \sqrt{p_n}$, por lo que (20) implica

$$\sqrt{p_n} < \frac{12}{e} n.$$

Por consiguiente

$$\frac{1}{2} \log p_n < \log n + \log \frac{12}{e}$$

que, substituido en (20), nos da

$$p_n < 6n \left(2 \log n + 2 \log \frac{12}{e} \right).$$

Esto demuestra la acotación superior de (19). □

Nota. La cota superior de (19) prueba una vez más que la serie

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

diverge, comparándola con $\sum_{n=2}^{\infty} 1/(n \log n)$.

4.6 TEOREMA TAUBERIANO DE SHAPIRO

Hemos demostrado que el teorema del número primo es equivalente a la fórmula asintótica

$$(21) \quad \frac{1}{x} \sum_{n \leq x} \Lambda(n) \sim 1 \quad \text{cuando } x \rightarrow \infty.$$

En el teorema 3.15 hemos obtenido una fórmula asintótica asociada,

$$(22) \quad \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = x \log x - x + O(\log x).$$

Las sumas de (21) y (22) son medias ponderadas de la función $\Lambda(n)$. Cada término $\Lambda(n)$ se halla multiplicado por un factor de peso $1/x$ en (21) y por $[x/n]$ en (22).

Los teoremas que relacionan diferentes medias ponderadas de una misma función se llaman *teoremas tauberianos*. A continuación discutiremos un teorema tauberiano demostrado en 1950 por H. N. Shapiro [64]. Relaciona sumas de la forma $\sum_{n \leq x} a(n)$ con sumas de la forma $\sum_{n \leq x} a(n) [x/n]$ para $a(n)$ no negativo.

Teorema 4.8 Sea $\{a(n)\}$ una sucesión no negativa tal que

$$(23) \quad \sum_{n \leq x} a(n) \left\lfloor \frac{x}{n} \right\rfloor = x \log x + O(x) \quad \text{para todo } x \geq 1.$$

Entonces:

(a) Para $x \geq 1$ tenemos

$$\sum_{n \leq x} \frac{a(n)}{n} = \log x + O(1).$$

(Con otras palabras, si borramos los corchetes de (23) obtenemos un resultado correcto.)

(b) Existe una constante $B > 0$ tal que

$$\sum_{n \leq x} a(n) \leq Bx \quad \text{para todo } x \geq 1.$$

(c) Existe una constante $A > 0$ y un $x_0 > 0$ tales que

$$\sum_{n \leq x} a(n) \geq Ax \quad \text{para todo } x \geq x_0.$$

DEMOSTRACIÓN. Sean

$$S(x) = \sum_{n \leq x} a(n), \quad T(x) = \sum_{n \leq x} a(n) \left\lfloor \frac{x}{n} \right\rfloor.$$

En primer lugar demostraremos (b). Para ello establecemos la desigualdad

$$(24) \quad S(x) - S\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right).$$

Escribimos

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n \leq x} \left\lfloor \frac{x}{n} \right\rfloor a(n) - 2 \sum_{n \leq x/2} \left\lfloor \frac{x}{2n} \right\rfloor a(n) \\ &= \sum_{n \leq x/2} \left(\left\lfloor \frac{x}{n} \right\rfloor - 2 \left\lfloor \frac{x}{2n} \right\rfloor \right) a(n) + \sum_{x/2 < n \leq x} \left\lfloor \frac{x}{n} \right\rfloor a(n). \end{aligned}$$

Puesto que $[2y] - 2[y]$ es 0 ó 1, la primera suma es no negativa, o sea

$$T(x) - 2T\left(\frac{x}{2}\right) \geq \sum_{x/2 < n \leq x} \left[\frac{x}{n}\right] a(n) = \sum_{x/2 < n \leq x} a(n) = S(x) - S\left(\frac{x}{2}\right).$$

Esto prueba (24). Pero (23) implica

$$T(x) - 2T\left(\frac{x}{2}\right) = x \log x + O(x) - 2\left(\frac{x}{2} \log \frac{x}{2} + O(x)\right) = O(x).$$

Por lo tanto (24) implica $S(x) - S(x/2) = O(x)$. Lo que asegura la existencia de una constante $K > 0$ tal que

$$S(x) - S\left(\frac{x}{2}\right) \leq Kx \quad \text{para todo } x \geq 1.$$

Substituimos, sucesivamente, x por $x/2, x/4, \dots$ y obtenemos

$$S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) \leq K \frac{x}{2},$$

$$S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) \leq K \frac{x}{4},$$

etcétera. Observamos que $S(x/2^n) = 0$ cuando $2^n \geq x$. Sumando estas desigualdades obtenemos

$$S(x) \leq Kx \left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) = 2Kx.$$

Esto demuestra (b) con $B = 2K$.

Ahora probaremos (a). Escribimos $[x/n] = (x/n) + O(1)$ y obtenemos

$$\begin{aligned} T(x) &= \sum_{n \leq x} \left[\frac{x}{n}\right] a(n) = \sum_{n \leq x} \left(\frac{x}{n} + O(1)\right) a(n) = x \sum_{n \leq x} \frac{a(n)}{n} + O\left(\sum_{n \leq x} a(n)\right) \\ &= x \sum_{n \leq x} \frac{a(n)}{n} + O(x), \end{aligned}$$

en virtud de la parte (b). Por lo tanto

$$\sum_{n \leq x} \frac{a(n)}{n} = \frac{1}{x} T(x) + O(1) = \log x + O(1).$$

Esto demuestra (a).

Finalmente, probaremos (c). Sea

$$A(x) = \sum_{n \leq x} \frac{a(n)}{n}.$$

Entonces (a) se puede escribir como sigue:

$$A(x) = \log x + R(x),$$

en donde $R(x)$ es el término de error. Puesto que $R(x) = O(1)$ tenemos $|R(x)| \leq M$ para un cierto $M > 0$.

Elegimos α que satisfaga $0 < \alpha < 1$ (en un cierto momento especificaremos α más exactamente) y consideramos la diferencia

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leq x} \frac{a(n)}{n} = \sum_{n \leq x} \frac{a(n)}{n} - \sum_{n \leq \alpha x} \frac{a(n)}{n}.$$

Si $x \geq 1$ y $\alpha x \geq 1$ podemos aplicar la fórmula asintótica relativa a $A(x)$ y escribir

$$\begin{aligned} A(x) - A(\alpha x) &= \log x + R(x) - (\log \alpha x + R(\alpha x)) \\ &= -\log \alpha + R(x) - R(\alpha x) \\ &\geq -\log \alpha - |R(x)| - |R(\alpha x)| \geq -\log \alpha - 2M. \end{aligned}$$

Ahora elegimos α tal que $-\log \alpha - 2M = 1$. Esto requiere que $\log \alpha = -2M - 1$, o $\alpha = e^{-2M-1}$. Obsérvese que $0 < \alpha < 1$. Para este α , tenemos la desigualdad

$$A(x) - A(\alpha x) \geq 1 \quad \text{si } x \geq 1/\alpha.$$

Pero

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leq x} \frac{a(n)}{n} \leq \frac{1}{\alpha x} \sum_{n \leq x} a(n) = \frac{S(x)}{\alpha x}.$$

Luego

$$\frac{S(x)}{\alpha x} \geq 1 \quad \text{si } x \geq 1/\alpha.$$

Por consiguiente $S(x) \geq \alpha x$ si $x \geq 1/\alpha$, que prueba (c) con $A = \alpha$ y $x_0 = 1/\alpha$. $\square$

4.7 APLICACIONES DEL TEOREMA DE SHAPIRO

La ecuación (22) implica

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = x \log x + O(x).$$

Puesto que $\Lambda(n) \geq 0$ podemos aplicar el teorema de Shapiro con $a(n) = \Lambda(n)$ para obtener:

Teorema 4.9 *Para todo $x \geq 1$ tenemos*

$$(25) \quad \sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

Por consiguiente, existen dos constantes positivas c_1 y c_2 tales que

$$\psi(x) \leq c_1 x \quad \text{para todo } x \geq 1$$

y

$$\psi(x) \geq c_2 x \quad \text{para todo } x \text{ suficientemente grande.}$$

A partir de la fórmula asintótica demostrada en el teorema 3.16

$$\sum_{p \leq x} \left[\frac{x}{p} \right] \log p = x \log x + O(x)$$

podemos obtener otra aplicación. Dicha fórmula asintótica se puede escribir en la forma

$$(26) \quad \sum_{n \leq x} \Lambda_1(n) \left[\frac{x}{n} \right] = x \log x + O(x),$$

en donde Λ_1 es la función definida como sigue:

$$\Lambda_1(n) = \begin{cases} \log p & \text{si } n \text{ es un primo } p, \\ 0 & \text{en otro caso.} \end{cases}$$

Puesto que $\Lambda_1(n) \geq 0$, la ecuación (26) prueba que se satisfacen las hipótesis del teorema de Shapiro con $a(n) = \Lambda_1(n)$. Puesto que $\vartheta(x) = \sum_{n \leq x} \Lambda_1(n)$, la parte (a) del teorema de Shapiro nos proporciona la siguiente fórmula asintótica.

Teorema 4.10 *Para todo $x \geq 1$ tenemos*

$$(27) \quad \sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Por consiguiente, existen dos constantes positivas c_1 y c_2 tales que

$$\vartheta(x) \leq c_1 x \quad \text{para todo } x \geq 1$$

y

$$\vartheta(x) \geq c_2 x \quad \text{para todo } x \text{ suficientemente grande.}$$

En el teorema 3.11 hemos demostrado que

$$\sum_{n \leq x} f(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} F\left(\frac{x}{n}\right)$$

para toda función aritmética $f(n)$ con sumas parciales $F(x) = \sum_{n \leq x} f(n)$. Dado que $\psi(x) = \sum_{n \leq x} \Lambda(n)$ y $\vartheta(x) = \sum_{n \leq x} \Lambda_1(n)$ resulta que las fórmulas asintóticas de (22) y (26) se pueden expresar directamente en términos de $\psi(x)$ y $\vartheta(x)$. Vamos a establecerlo como teorema formal.

Teorema 4.11 *Para todo $x \geq 1$ tenemos*

$$(28) \quad \sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x)$$

y

$$\sum_{n \leq x} \vartheta\left(\frac{x}{n}\right) = x \log x + O(x).$$

4.8 UNA FÓRMULA ASINTÓTICA PARA LAS SUMAS PARCIALES

$$\sum_{p \leq x} (1/p)$$

En el capítulo 1 veíamos que la serie $\sum (1/p)$ diverge. Ahora obtenemos una fórmula asintótica para sus sumas parciales. El resultado es una aplicación del teorema 4.10, ecuación (27).

Teorema 4.12 *Existe una constante A tal que*

$$(29) \quad \sum_{p \leq x} \frac{1}{p} = \log \log x + A + O\left(\frac{1}{\log x}\right) \quad \text{para todo } x \geq 2.$$

DEMOSTRACIÓN. Sea

$$A(x) = \sum_{p \leq x} \frac{\log p}{p}$$

y sea

$$a(n) = \begin{cases} 1 & \text{si } n \text{ es primo,} \\ 0 & \text{en otro caso.} \end{cases}$$

Entonces

$$\sum_{p \leq x} \frac{1}{p} = \sum_{n \leq x} \frac{a(n)}{n} \quad \text{y} \quad A(x) = \sum_{n \leq x} \frac{a(n)}{n} \log n.$$

Por consiguiente, si en el teorema 4.2 hacemos $f(t) = 1/\log t$, obtenemos, ya que $A(t) = 0$ para $t < 2$,

$$(30) \quad \sum_{p \leq x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t \log^2 t} dt.$$

De (27) tenemos $A(x) = \log x + R(x)$, en donde $R(x) = O(1)$. Utilizando este resultado en el segundo miembro de (30) obtenemos

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \frac{\log x + O(1)}{\log x} + \int_2^x \frac{\log t + R(t)}{t \log^2 t} dt \\ (31) \quad &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t \log t} + \int_2^x \frac{R(t)}{t \log^2 t} dt. \end{aligned}$$

Ahora bien

$$\int_2^x \frac{dt}{t \log t} = \log \log x - \log \log 2$$

y

$$\int_2^x \frac{R(t)}{t \log^2 t} dt = \int_2^\infty \frac{R(t)}{t \log^2 t} dt - \int_x^\infty \frac{R(t)}{t \log^2 t} dt,$$

en donde la existencia de la integral impropia está asegurada por la condición $R(t) = O(1)$. Pero

$$\int_x^\infty \frac{R(t)}{t \log^2 t} dt = O\left(\int_x^\infty \frac{dt}{t \log^2 t}\right) = O\left(\frac{1}{\log x}\right).$$

Luego la ecuación (31) se puede escribir como sigue:

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + 1 - \log \log 2 + \int_2^\infty \frac{R(t)}{t \log^2 t} dt + O\left(\frac{1}{\log x}\right).$$

Esto demuestra el teorema con

$$A = 1 - \log \log 2 + \int_2^\infty \frac{R(t)}{t \log^2 t} dt. \quad \square$$

4.9 LAS SUMAS PARCIALES DE LA FUNCIÓN DE MÖBIUS

Definición. Si $x \geq 1$ definimos

$$M(x) = \sum_{n \leq x} \mu(n).$$

El orden exacto de magnitud de $M(x)$ se desconoce. Evidencias numéricas sugieren que

$$|M(x)| < \sqrt{x} \quad \text{si } x > 1,$$

pero esta desigualdad, conocida como conjetura de Mertens, no ha sido demostrada ni desmentida. El mejor O -resultado obtenido hasta el momento es

$$M(x) = O(x\delta(x))$$

en donde $\delta(x) = \exp \{ -A \log^{3/5} x (\log \log x)^{-1/5} \}$ para una cierta constante positiva A . (En Walfisz [75] se da una demostración.)

En esta sección probaremos que la proposición débil

$$\lim_{x \rightarrow \infty} \frac{M(x)}{x} = 0$$

es equivalente al teorema del número primo. En primer lugar relacionaremos $M(x)$ con otra media ponderada de $\mu(n)$.

Definición. Si $x \geq 1$ definimos

$$H(x) = \sum_{n \leq x} \mu(n) \log n.$$

El teorema que sigue prueba que el comportamiento de $M(x)/x$ se halla determinado por el de $H(x)/(x \log x)$.

Teorema 4.13 *Tenemos*

$$(32) \quad \lim_{x \rightarrow \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0.$$

DEMOSTRACIÓN. Si hacemos $f(t) = \log t$ en el teorema 4.2 obtenemos

$$H(x) = \sum_{n \leq x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t} dt.$$

Luego, si $x > 1$, tenemos

$$\frac{M(x)}{x} - \frac{H(x)}{x \log x} = \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt.$$

Por consiguiente para demostrar el teorema debemos establecer que

$$(33) \quad \lim_{x \rightarrow \infty} \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt = 0.$$

Pero disponemos de la estimación trivial $M(x) = O(x)$, luego

$$\int_1^x \frac{M(t)}{t} dt = O\left(\int_1^x dt\right) = O(x),$$

de donde se obtiene (33), y por lo tanto (32). □

Teorema 4.14 *El teorema del número primo implica*

$$\lim_{x \rightarrow \infty} \frac{M(x)}{x} = 0.$$

DEMOSTRACIÓN. Utilizamos el teorema del número primo en la forma $\psi(x) \sim x$ y vemos que $H(x)/(x \log x) \rightarrow 0$ cuando $x \rightarrow \infty$. A este fin estableceremos la identidad

$$(34) \quad -H(x) = - \sum_{n \leq x} \mu(n) \log n = \sum_{n \leq x} \mu(n) \psi\left(\frac{x}{n}\right).$$

Para probar (34) empezamos con el teorema 2.11 que establece

$$\Lambda(n) = - \sum_{d|n} \mu(d) \log d$$

y aplicamos la inversión de Möbius para obtener

$$-\mu(n)\log n = \sum_{d|n} \mu(d) \Lambda\left(\frac{n}{d}\right).$$

Si sumamos con respecto a $n \leq x$ y usamos el teorema 3.10 con $f = \mu$, $g = \Lambda$, obtenemos (34).

Puesto que $\psi(x) \sim x$, dado un $\varepsilon > 0$, existe una constante $A > 0$ tal que

$$\left| \frac{\psi(x)}{x} - 1 \right| < \varepsilon \quad \text{siempre que } x \geq A.$$

Por consiguiente,

$$(35) \quad |\psi(x) - x| < \varepsilon x \quad \text{siempre que } x \geq A.$$

Elegimos $x > A$ y descomponemos la suma de la derecha de (34) en dos partes,

$$\sum_{n \leq y} + \sum_{y < n \leq x},$$

en donde $y = [x/A]$. En la primera suma tenemos $n \leq y$ o sea $n \leq x/A$, y por lo tanto $x/n \geq A$. Por consiguiente podemos utilizar (35) para escribir

$$\left| \psi\left(\frac{x}{n}\right) - \frac{x}{n} \right| < \varepsilon \frac{x}{n} \quad \text{si } n \leq y.$$

Entonces,

$$\begin{aligned} \sum_{n \leq y} \mu(n) \psi\left(\frac{x}{n}\right) &= \sum_{n \leq y} \mu(n) \left(\frac{x}{n} + \psi\left(\frac{x}{n}\right) - \frac{x}{n} \right) \\ &= x \sum_{n \leq y} \frac{\mu(n)}{n} + \sum_{n \leq y} \mu(n) \left(\psi\left(\frac{x}{n}\right) - \frac{x}{n} \right), \end{aligned}$$

o sea

$$\left| \sum_{n \leq y} \mu(n) \psi\left(\frac{x}{n}\right) \right| \leq x \left| \sum_{n \leq y} \frac{\mu(n)}{n} \right| + \sum_{n \leq y} \left| \psi\left(\frac{x}{n}\right) - \frac{x}{n} \right|$$

$$\begin{aligned}
 &< x + \varepsilon \sum_{n \leq y} \frac{x}{n} < x + \varepsilon x(1 + \log y) \\
 &< x + \varepsilon x + \varepsilon x \log x.
 \end{aligned}$$

En la segunda suma tenemos $y < n \leq x$ o sea $n \geq y + 1$. Por tanto

$$\frac{x}{n} \leq \frac{x}{y+1} < A$$

puesto que

$$y \leq \frac{x}{A} < y + 1.$$

La desigualdad $(x/n) < A$ implica $\psi(x/n) \leq \psi(A)$. Por consiguiente la segunda suma está dominada por $x\psi(A)$. Por consiguiente la suma entera de (34) está dominada por

$$(1 + \varepsilon)x + \varepsilon x \log x + x\psi(A) < (2 + \psi(A))x + \varepsilon x \log x$$

si $\varepsilon < 1$. Con otras palabras, dado un ε tal que $0 < \varepsilon < 1$, tenemos

$$|H(x)| < (2 + \psi(A))x + \varepsilon x \log x \quad \text{si } x > A,$$

luego

$$\frac{|H(x)|}{x \log x} < \frac{2 + \psi(A)}{\log x} + \varepsilon.$$

Ahora elegimos $B > A$ de manera que $x > B$ implica $(2 + \psi(A))/\log x < \varepsilon$. Entonces para $x > B$ tenemos

$$\frac{|H(x)|}{x \log x} < 2\varepsilon,$$

que demuestra que $H(x)/(x \log x) \rightarrow 0$ cuando $x \rightarrow \infty$. □

Volvemos al recíproco del teorema 4.14 y probamos que la relación

$$(36) \quad \lim_{x \rightarrow \infty} \frac{M(x)}{x} = 0$$

implica el teorema del número primo. En primer lugar introducimos la notación de la «o minúscula».

Definición. La notación

$$f(x) = o(g(x)) \quad \text{cuando } x \rightarrow \infty \quad (\text{léase: } f(x) \text{ es o minúscula de } g(x))$$

significa que

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0.$$

Una ecuación de la forma

$$f(x) = h(x) + o(g(x)) \quad \text{cuando } x \rightarrow \infty$$

significa que $f(x) - h(x) = o(g(x))$ cuando $x \rightarrow \infty$.

Así pues, (36) establece que

$$M(x) = o(x) \quad \text{cuando } x \rightarrow \infty,$$

y el teorema del número primo, expresado en la forma $\psi(x) \sim x$, se puede escribir también en la forma

$$\psi(x) = x + o(x) \quad \text{cuando } x \rightarrow \infty.$$

Con más generalidad, una relación asintótica

$$f(x) \sim g(x) \quad \text{cuando } x \rightarrow \infty$$

es equivalente a

$$f(x) = g(x) + o(g(x)) \quad \text{cuando } x \rightarrow \infty.$$

Observemos también que $f(x) = O(1)$ implica $f(x) = o(x)$ cuando $x \rightarrow \infty$.

Teorema 4.15 *La relación*

$$(37) \quad M(x) = o(x) \quad \text{cuando } x \rightarrow \infty$$

implica $\psi(x) \sim x$ cuando $x \rightarrow \infty$.

DEMOSTRACIÓN. En primer lugar expresamos $\psi(x)$ por medio de una fórmula del tipo

$$(38) \quad \psi(x) = x - \sum_{\substack{q, d \\ qd \leq x}} \mu(d)f(q) + O(1)$$

y entonces utilizamos (37) para demostrar que la suma es $o(x)$ cuando $x \rightarrow \infty$. La función f de (38) viene dada por

$$f(n) = \sigma_0(n) - \log n - 2C,$$

en donde C es la constante de Euler y $\sigma_0(n) = d(n)$ es el número de divisores de n . Para obtener (38) partimos de las identidades

$$[x] = \sum_{n \leq x} 1, \quad \psi(x) = \sum_{n \leq x} \Lambda(n), \quad 1 = \sum_{n \leq x} \left[\frac{1}{n} \right]$$

y expresamos cada sumando como un producto de Dirichlet que contiene la función de Möbius,

$$1 = \sum_{d|n} \mu(d) \sigma_0\left(\frac{n}{d}\right), \quad \Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d}, \quad \left[\frac{1}{n} \right] = \sum_{d|n} \mu(d).$$

Entonces

$$\begin{aligned} [x] - \psi(x) - 2C &= \sum_{n \leq x} \left\{ 1 - \Lambda(n) - 2C \left[\frac{1}{n} \right] \right\} \\ &= \sum_{n \leq x} \sum_{d|n} \mu(d) \left\{ \sigma_0\left(\frac{n}{d}\right) - \log \frac{n}{d} - 2C \right\} \\ &= \sum_{\substack{q, d \\ qd \leq x}} \mu(d) \{ \sigma_0(q) - \log q - 2C \} \\ &= \sum_{\substack{q, d \\ qd \leq x}} \mu(d) f(q). \end{aligned}$$

Esto implica (38). Por consiguiente la demostración del teorema quedará establecida si demostramos que

$$(39) \quad \sum_{\substack{q, d \\ qd \leq x}} \mu(d)f(q) = o(x) \quad \text{cuando } x \rightarrow \infty.$$

A este fin utilizamos el teorema 3.17 para escribir

$$(40) \quad \sum_{\substack{q, d \\ qd \leq x}} \mu(d)f(q) = \sum_{n \leq b} \mu(n)F\left(\frac{x}{n}\right) + \sum_{n \leq a} f(n)M\left(\frac{x}{n}\right) - F(a)M(b)$$

en donde a y b son números positivos tales que $ab = x$ y

$$F(x) = \sum_{n \leq x} f(n).$$

A continuación probaremos que $F(x) = O(\sqrt{x})$ utilizando la fórmula de Dirichlet (teorema 3.3)

$$\sum_{n \leq x} \sigma_0(n) = x \log x + (2C - 1)x + O(\sqrt{x})$$

junto con la relación

$$\sum_{n \leq x} \log n = \log[x]! = x \log x - x + O(\log x).$$

Esto nos proporciona

$$\begin{aligned} F(x) &= \sum_{n \leq x} \sigma_0(n) - \sum_{n \leq x} \log n - 2C \sum_{n \leq x} 1 \\ &= x \log x + (2C - 1)x + O(\sqrt{x}) - (x \log x - x + O(\log x)) \\ &\quad - 2Cx + O(1) \\ &= O(\sqrt{x}) + O(\log x) + O(1) = O(\sqrt{x}). \end{aligned}$$

Por consiguiente existe una constante $B > 0$ tal que

$$|F(x)| \leq B\sqrt{x} \quad \text{para todo } x \geq 1.$$

Utilizando este resultado en la primera suma de la derecha de (40) obtenemos

$$(41) \quad \left| \sum_{n \leq b} \mu(n) F\left(\frac{x}{n}\right) \right| \leq B \sum_{n \leq b} \sqrt{\frac{x}{n}} \leq A \sqrt{xb} = \frac{Ax}{\sqrt{a}}$$

para una constante $A > B > 0$.

Sea ahora un $\varepsilon > 0$ arbitrario y elijamos un $a > 1$ tal que

$$\frac{A}{\sqrt{a}} < \varepsilon.$$

Entonces (41) conduce a

$$(42) \quad \left| \sum_{n \leq b} \mu(n) F\left(\frac{x}{n}\right) \right| < \varepsilon x$$

para todo $x \geq 1$. Obsérvese que a depende de ε pero no depende de x .

Puesto que $M(x) = O(x)$ cuando $x \rightarrow \infty$, para el mismo ε existe un $c > 0$ (que únicamente depende de ε) tal que

$$x > c \text{ implica } \frac{|M(x)|}{x} < \frac{\varepsilon}{K},$$

en donde K es un cierto número positivo. (Seguidamente precisaremos K .) La segunda suma de la derecha de (40) satisface

$$(43) \quad \left| \sum_{n \leq a} f(n) M\left(\frac{x}{n}\right) \right| \leq \sum_{n \leq a} |f(n)| \frac{\varepsilon x}{K n} = \frac{\varepsilon x}{K} \sum_{n \leq a} \frac{|f(n)|}{n}$$

si suponemos que, para todo $n \leq a$, $x/n > c$. Por consiguiente (43) se verifica si $x > ac$. Ahora tomamos

$$K = \sum_{n \leq a} \frac{|f(n)|}{n}.$$

Entonces (43) implica

$$(44) \quad \left| \sum_{n \leq a} f(n) M\left(\frac{x}{n}\right) \right| < \varepsilon x \text{ en el supuesto de que } x > ac.$$

El último término de la derecha de (40) se halla dominado por

$$|F(a)M(b)| \leq A\sqrt{a} |M(b)| < A\sqrt{ab} < \varepsilon\sqrt{b}\sqrt{ab} = \varepsilon\sqrt{x}b < \varepsilon x$$

en el supuesto de que $\sqrt{x} > a$, o $x > a^2$. Combinando esto con (44) y (42) vemos que (40) implica

$$\left| \sum_{\substack{q, d \\ qd \leq x}} \mu(d)f(q) \right| < 3\varepsilon x$$

en el supuesto de que $x > a^2$ y $x > ac$, en donde a y c únicamente dependen de ε . Esto prueba (39). $\square$

Teorema 4.16 Si

$$A(x) = \sum_{n \leq x} \frac{\mu(n)}{n}$$

la relación

$$(45) \quad A(x) = o(1) \quad \text{cuando } x \rightarrow \infty$$

implica el teorema del número primo. Con otras palabras, el teorema del número primo es una consecuencia de la afirmación que establece que la serie

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$$

converge y tiene suma 0.

Nota. Podemos demostrar asimismo (ver [3]) que el teorema del número primo implica la convergencia de esta serie hacia 0, o sea (45) realmente equivale al teorema del número primo.

DEMOSTRACIÓN. Probaremos que (45) implica $M(x) = o(x)$. Por la identidad de Abel tenemos

$$M(x) = \sum_{n \leq x} \mu(n) = \sum_{n \leq x} \frac{\mu(n)}{n} n = xA(x) - \int_1^x A(t) dt,$$

o sea

$$\frac{M(x)}{x} = A(x) - \frac{1}{x} \int_1^x A(t) dt.$$

Por consiguiente, para completar la demostración basta probar que

$$(46) \quad \lim_{x \rightarrow \infty} \frac{1}{x} \int_1^x A(t) dt = 0.$$

Ahora bien, dado $\varepsilon > 0$ existe un c (que únicamente depende de ε) tal que $|A(x)| < \varepsilon$ si $x \geq c$. Puesto que $|A(x)| \leq 1$ para todo $x \geq 1$ tenemos

$$\left| \frac{1}{x} \int_1^x A(t) dt \right| \leq \left| \frac{1}{x} \int_1^c A(t) dt \right| + \left| \frac{1}{x} \int_c^x A(t) dt \right| \leq \frac{c-1}{x} + \frac{\varepsilon(x-c)}{x}.$$

Si hacemos que $x \rightarrow \infty$ obtenemos

$$\limsup_{x \rightarrow \infty} \left| \frac{1}{x} \int_1^x A(t) dt \right| \leq \varepsilon,$$

y dado que ε es arbitrario resulta (46). □

4.10 BREVE ESBOZO DE UNA DEMOSTRACIÓN ELEMENTAL DEL TEOREMA DEL NÚMERO PRIMO

En esta sección se da un esbozo de una demostración elemental del teorema del número primo. Para completar detalles puede recurrirse a [31] o a [46]. El meollo de esta demostración lo constituye una fórmula asintótica de Selberg que establece que

$$\psi(x) \log x + \sum_{n \leq x} \Lambda(n) \psi\left(\frac{x}{n}\right) = 2x \log x + O(x).$$

La demostración de la fórmula de Selberg es relativamente simple y se da en la sección que sigue. Esta sección perfila los pasos principales utilizados para deducir de la fórmula de Selberg el teorema del número primo.

En primer lugar, la fórmula de Selberg se expresa en una forma mucho más conveniente que contiene a la función

$$\sigma(x) = e^{-x}\psi(e^x) - 1.$$

La fórmula de Selberg implica una desigualdad integral de la forma

$$(47) \quad |\sigma(x)|x^2 \leq 2 \int_0^x \int_0^y |\sigma(u)| du dy + O(x),$$

y el teorema del número primo equivale a demostrar que $\sigma(x) \rightarrow 0$ cuando $x \rightarrow \infty$. Por consiguiente, si hacemos

$$C = \limsup_{x \rightarrow \infty} |\sigma(x)|,$$

el teorema del número primo equivale a demostrar que $C = 0$. Se demuestra suponiendo que $C > 0$ y se obtiene, como sigue, una contradicción. En virtud de la definición de C tenemos

$$(48) \quad |\sigma(x)| \leq C + g(x),$$

en donde $g(x) \rightarrow 0$ cuando $x \rightarrow \infty$. Si $C > 0$, esta desigualdad junto con (47) nos proporciona otra desigualdad del mismo tipo,

$$(49) \quad |\sigma(x)| \leq C' + h(x),$$

en donde $0 < C' < C$ y $h(x) \rightarrow 0$ cuando $x \rightarrow \infty$. La deducción de (49) a partir de (47) y (48) es la parte más larga de la demostración. Si en (49) hacemos que $x \rightarrow \infty$ obtenemos que $C \leq C'$, y esta contradicción establece el teorema.

4.11 FÓRMULA ASINTÓTICA DE SELBERG

Deduciremos la fórmula de Selberg utilizando un método dado por Tatzuwa e Iseki [68] en 1951. Se basa en el teorema que sigue que tiene la naturaleza de una fórmula de inversión.

Teorema 4.17 *Sea F una función a valores reales —o complejos— definida en $(0, \infty)$, y sea*

$$G(x) = \log x \sum_{n \leq x} F\left(\frac{x}{n}\right).$$

Entonces

$$F(x)\log x + \sum_{n \leq x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{d \leq x} \mu(d)G\left(\frac{x}{d}\right).$$

DEMOSTRACIÓN. Primero escribiremos $F(x)\log x$ como una suma,

$$F(x)\log x = \sum_{n \leq x} \left[\frac{1}{n} \right] F\left(\frac{x}{n}\right) \log \frac{x}{n} = \sum_{n \leq x} F\left(\frac{x}{n}\right) \log \frac{x}{n} \sum_{d|n} \mu(d)$$

y luego utilizaremos la identidad del teorema 2.11,

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d}$$

para escribir

$$\sum_{n \leq x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n \leq x} F\left(\frac{x}{n}\right) \sum_{d|n} \mu(d) \log \frac{n}{d}.$$

Sumando estas ecuaciones obtenemos

$$\begin{aligned} F(x)\log x + \sum_{n \leq x} F\left(\frac{x}{n}\right)\Lambda(n) &= \sum_{n \leq x} F\left(\frac{x}{n}\right) \sum_{d|n} \mu(d) \left\{ \log \frac{x}{n} + \log \frac{n}{d} \right\} \\ &= \sum_{n \leq x} \sum_{d|n} F\left(\frac{x}{n}\right) \mu(d) \log \frac{x}{d}. \end{aligned}$$

En la última suma escribimos $n = qd$ a fin de obtener

$$\sum_{n \leq x} \sum_{d|n} F\left(\frac{x}{n}\right) \mu(d) \log \frac{x}{d} = \sum_{d \leq x} \mu(d) \log \frac{x}{d} \sum_{q \leq x/d} F\left(\frac{x}{qd}\right) = \sum_{d \leq x} \mu(d) G\left(\frac{x}{d}\right),$$

que establece la demostración del teorema. □

Teorema 4.18 Fórmula asintótica de Selberg. Para $x > 0$ tenemos

$$\psi(x) \log x + \sum_{n \leq x} \Lambda(n) \psi\left(\frac{x}{n}\right) = 2x \log x + O(x).$$

DEMOSTRACIÓN. Aplicamos el teorema 4.17 a la función $F_1(x) = \psi(x)$ y también a $F_2(x) = x - C - 1$, en donde C es la constante de Euler. En correspondencia con F_1 tenemos

$$G_1(x) = \log x \sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log^2 x - x \log x + O(\log^2 x),$$

en donde hemos utilizado el teorema 4.11. En correspondencia con F_2 tenemos

$$\begin{aligned} G_2(x) &= \log x \sum_{n \leq x} F_2\left(\frac{x}{n}\right) = \log x \sum_{n \leq x} \left(\frac{x}{n} - C - 1\right) \\ &= x \log x \sum_{n \leq x} \frac{1}{n} - (C + 1) \log x \sum_{n \leq x} 1 \\ &= x \log x \left(\log x + C + O\left(\frac{1}{x}\right) \right) - (C + 1) \log x (x + O(1)) \\ &= x \log^2 x - x \log x + O(\log x). \end{aligned}$$

Comparando las fórmulas relativas a $G_1(x)$ y a $G_2(x)$ vemos que $G_1(x) - G_2(x) = O(\log^2 x)$. De hecho, únicamente utilizaremos la estimación débil

$$G_1(x) - G_2(x) = O(\sqrt{x}).$$

Ahora aplicamos el teorema 4.17 a cada una de las funciones F_1 y F_2 y restamos las dos relaciones así obtenidas. La diferencia de los dos primeros miembros es

$$\sum_{d \leq x} \mu(d) \left\{ G_1\left(\frac{x}{d}\right) - G_2\left(\frac{x}{d}\right) \right\} = O\left(\sum_{d \leq x} \sqrt{\frac{x}{d}} \right) = O\left(\sqrt{x} \sum_{d \leq x} \frac{1}{\sqrt{d}} \right) = O(x)$$

en virtud del teorema 3.2(b). Por consiguiente la diferencia de los dos segundos miembros es también $O(x)$. Con otras palabras, tenemos

$$\{\psi(x) - (x - C - 1)\} \log x + \sum_{n \leq x} \left\{ \psi\left(\frac{x}{n}\right) - \left(\frac{x}{n} - C - 1\right) \right\} \Lambda(n) = O(x).$$

Reordenando términos y utilizando el teorema 4.9 resulta

$$\begin{aligned} \psi(x) \log x + \sum_{n \leq x} \psi\left(\frac{x}{n}\right) \Lambda(n) &= (x - C - 1) \log x \\ &+ \sum_{n \leq x} \left(\frac{x}{n} - C - 1\right) \Lambda(n) + O(x) \\ &= 2x \log x + O(x). \end{aligned} \quad \square$$

Ejercicio del capítulo 4

- Sea $S = \{1, 5, 9, 13, 17, \dots\}$ el conjunto de todos los enteros positivos de la forma $4n + 1$. Un elemento p de S se llama un S -primo si $p > 1$ y si los únicos divisores de p , que pertenecen a S son 1 y p . (Por ejemplo, 49 es un S -primo.) Un elemento $n > 1$ de S que no es S -primo se llama S -compuesto.
 - Probar que cada S -compuesto es producto de S -primos.
 - Buscar el menor S -compuesto que se puede escribir de varias formas como producto de S -primos.
 Este ejemplo demuestra que en S no se verifica la unicidad de la descomposición.
- Consideremos el siguiente conjunto finito de enteros:

$$T = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$

- Cada primo p del intervalo $30 < p < 100$ determina un par de enteros m, n en donde $m \geq 0$ y $n \in T$, tal que $p = 30m + n$.
 - Mostrar la proposición que sigue o dar un contraejemplo:
Cada primo $p > 5$ se puede expresar en la forma $30m + n$, en donde $m \geq 0$ y $n \in T$.
- Sea $f(x) = x + x + 41$. Buscar el menor entero $x \geq 0$ para el que $f(x)$ es compuesto.
 - Sea $f(x) = a_0 + a_1x + \dots + a_nx^n$ un polinomio con coeficientes enteros, tal que $a_n > 0$ y $n \geq 1$. Probar que $f(x)$ es compuesto para una infinidad de enteros x .
 - Probar que, para cada $n > 1$, existen n números compuestos consecutivos.
 - Probar que no existen polinomios P y Q tales que

$$\pi(x) = \frac{P(x)}{Q(x)} \quad \text{para } x = 1, 2, 3, \dots$$

7. Sea $a_1 < a_2 < \dots < a_n \leq x$ un conjunto de enteros positivos tales que ningún a_i divida al producto de los otros. Probar que $n \leq \pi(x)$.
8. Calcular la mayor potencia de 10 que divide a 1000!
9. Dada una progresión aritmética de enteros

$$h, h + k, h + 2k, \dots, h + nk, \dots,$$

en donde $0 < k < 2000$. Si $h + nk$ es primo para $n = t, t + 1, \dots, t + r$, probar que $r \leq 9$. Con otras palabras, en esta progresión sólo son primos a lo sumo 10 términos consecutivos.

10. Si s_n designa la suma parcial n -ésima de la serie

$$\sum_{r=1}^{\infty} \frac{1}{r(r+1)}.$$

probar que cada entero $k > 1$ existen enteros m y n tales que $s_m - s_n = 1/k$.

11. Si s_n designa la suma de los n primeros primos, probar que, para cada n , existe un entero cuyo cuadrado se halla entre s_n y s_{n+1} .

Probar cada una de las afirmaciones contenidas en los ejercicios 12 al 16. En este grupo de ejercicios puede utilizarse el teorema del número primo.

12. Si $a > 0$ y $b > 0$, entonces $\pi(ax)/\pi(bx) \sim a/b$ cuando $x \rightarrow \infty$.
13. Si $0 < a < b$, existe un x_0 tal que $\pi(ax) < \pi(bx)$ si $x \geq x_0$.
14. Si $0 < a < b$, existe un x_0 tal que para $x \geq x_0$ existe un primo, por lo menos, entre ax y bx .
15. Cada intervalo $[a, b]$ con $0 < a < b$ contiene un número racional de la forma p/q , en donde p y q son primos.
16. (a) Dado un entero positivo n existe un entero positivo k y un primo p tal que $10^k_n < p < 10^{k(n+1)}$.
- (b) Dados m enteros $a_1, \dots, a_m$ tales que $0 \leq a_i \leq 9$ para $i = 1, 2, \dots, m$, existe un primo p cuya expresión decimal tiene a $a_1, \dots, a_m$ como m primeros dígitos.
17. Se da un entero $n > 1$ con dos descomposiciones $n = \prod_{i=1}^r p_i$ y $n = \prod_{i=1}^t q_i$, en donde los p_i son primos (no necesariamente distintos) y los q_i son enteros arbitrarios > 1 . Sea α un número real no negativo.
- (a) Si $\alpha \geq 1$ probar que

$$\sum_{i=1}^r p_i^\alpha \leq \sum_{i=1}^t q_i^\alpha.$$

- (b) Obtener una desigualdad que corresponda a la anterior y que relacione tales sumas en el caso de que $0 \leq \alpha < 1$.

18. Probar que las dos relaciones que siguen son equivalentes:

$$(a) \quad \pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

$$(b) \quad \vartheta(x) = x + O\left(\frac{x}{\log x}\right).$$

19. Si $x \geq 2$, sea

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t} \quad (\text{la integral logarítmica de } x).$$

(a) Probar que

$$\text{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2},$$

y que, en general,

$$\text{Li}(x) = \frac{x}{\log x} \left(1 + \sum_{k=1}^{n-1} \frac{k!}{\log^k x} \right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n,$$

en donde C_n es independiente de x .

(b) Si $x \geq 2$ probar que

$$\int_2^x \frac{dt}{\log^n t} = O\left(\frac{x}{\log^n x}\right).$$

20. Sea f una función aritmética tal que

$$\sum_{p \leq x} f(p) \log p = (ax + b) \log x + cx + O(1) \quad \text{para } x \geq 2.$$

Probar que existe una constante A (que depende de f) tal que, si $x \geq 2$,

$$\sum_{p \leq x} f(p) = ax + (a + c) \left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} \right) + b \log(\log x) + A + O\left(\frac{1}{\log x}\right).$$

21. Se dan dos funciones con valores reales $S(x)$ y $T(x)$ tales que

$$T(x) = \sum_{n \leq x} S\left(\frac{x}{n}\right) \quad \text{para todo } x \geq 1.$$

Si $S(x) = O(x)$ y, si c es una constante positiva, probar que la relación

$$S(x) \sim cx \quad \text{cuando } x \rightarrow \infty$$

implica

$$T(x) \sim cx \log x \quad \text{cuando } x \rightarrow \infty.$$

22. Probar que la fórmula de Selberg, tal como se expresa en el teorema 4.18, es equivalente a cada una de las relaciones que siguen:

$$(a) \quad \psi(x) \log x + \sum_{p \leq x} \psi\left(\frac{x}{p}\right) \log p = 2x \log x + O(x).$$

$$(b) \quad \vartheta(x) \log x + \sum_{p \leq x} \vartheta\left(\frac{x}{p}\right) \log p = 2x \log x + O(x).$$

23. Sea $M(x) = \sum_{n \leq x} \mu(n)$. Probar que

$$M(x) \log x + \sum_{n \leq x} M\left(\frac{x}{n}\right) \Lambda(n) = O(x)$$

y que

$$M(x) \log x + \sum_{p \leq x} M\left(\frac{x}{p}\right) \log p = O(x).$$

[Indicación: Teorema 4.17.]

24. Si $A(x)$ está definida para todo $x > 0$ y si suponemos que

$$T(x) = \sum_{n \leq x} A\left(\frac{x}{n}\right) = ax \log x + bx + o\left(\frac{x}{\log x}\right) \quad \text{cuando } x \rightarrow \infty,$$

en donde a y b son constantes, probar que

$$A(x) \log x + \sum_{n \leq x} A\left(\frac{x}{n}\right) \Lambda(n) = 2ax \log x + o(x \log x) \quad \text{cuando } x \rightarrow \infty.$$

Verificar que la fórmula de Selberg del teorema 4.18 es un caso especial.

25. Probar que el teorema del número primo en la forma $\psi(x) \sim x$ implica la fórmula asintótica de Selberg del teorema 4.18 con un término de error $o(x \log x)$ cuando $x \rightarrow \infty$.
26. En 1851 Chebyshev demostró que, si $\psi(x)/x$ tiene límite cuando $x \rightarrow \infty$ entonces este límite es igual a 1. Este ejercicio esboza una demostración simple basada en la fórmula

$$(50) \quad \sum_{n \leq x} \psi\left(\frac{x}{n}\right) = x \log x + O(x)$$

que se sigue del teorema 4.11.

- (a) Sea $\delta = \limsup_{x \rightarrow \infty} (\psi(x)/x)$. Dado un $\varepsilon > 0$, elegimos un $N = N(\varepsilon)$ tal que $x \geq N$ implique $\psi(x) \leq (\delta + \varepsilon)x$. Descomponer la suma de (50) en dos partes, una con $n \leq x/N$, la otra con $n > x/N$, y estimar cada parte a fin de obtener la desigualdad

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) \leq (\delta + \varepsilon)x \log x + x\psi(N).$$

Comparando este resultado con (50), deducir que $\delta \geq 1$.

- (b) Sea $\gamma = \liminf_{x \rightarrow \infty} (\psi(x)/x)$ y utilícese un argumento análogo al utilizado en (a) para deducir que $\gamma \leq 1$. Por consiguiente, si $\psi(x)/x$ tiene límite cuando $x \rightarrow \infty$, entonces $\gamma = \delta = 1$.

En los ejercicios que van del 27 al 30, sea $A(x) = \sum_{n \leq x} a(n)$, en donde $a(n)$ satisface

$$(51) \quad a(n) \geq 0 \quad \text{para todo } n \geq 1,$$

y

$$(52) \quad \sum_{n \leq x} A\left(\frac{x}{n}\right) = \sum_{n \leq x} a(n) \left[\frac{x}{n} \right] = ax \log x + bx + o\left(\frac{x}{\log x}\right) \quad \text{cuando } x \rightarrow \infty.$$

Cuando $a(n) = \Lambda(n)$, estas relaciones se verifican con $a = 1$ y $b = -1$. Los ejercicios que siguen prueban que (51) y (52), junto con el teorema del número primo, $\psi(x) \sim x$ implica $A(x) \sim ax$. Compárese este resultado con el teorema 4.8 (teorema tauberiano de Shapiro) que únicamente supone (51) y la condición más débil $\sum_{n \leq x} A(x/n) = ax \log x + O(x)$ y concluye que $Cx \leq A(x) \leq Bx$ para ciertas constantes positivas C y B .

27. Probar que

$$(a) \quad \sum_{n \leq x} A\left(\frac{x}{n}\right) \Lambda(n) = \sum_{n \leq \sqrt{x}} A\left(\frac{x}{n}\right) \Lambda(n) + \sum_{n \leq \sqrt{x}} \psi\left(\frac{x}{n}\right) a(n) + O(x)$$

y utilizar este resultado para deducir la relación

$$(b) \frac{A(x)}{x} + \frac{1}{x \log x} \sum_{n \leq \sqrt{x}} A\left(\frac{x}{n}\right) \Lambda(n) + \frac{1}{x \log x} \sum_{n \leq \sqrt{x}} \psi\left(\frac{x}{n}\right) a(n) = 2a + o(1).$$

28. Sea $\alpha = \liminf_{x \rightarrow \infty} (A(x)/x)$ y sea $\beta = \limsup_{x \rightarrow \infty} (A(x)/x)$.

(a) Elegir un $\varepsilon > 0$ y utilizar el hecho de que

$$A\left(\frac{x}{t}\right) < (\beta + \varepsilon) \frac{x}{t} \quad \text{y} \quad \psi\left(\frac{x}{t}\right) < (1 + \varepsilon) \frac{x}{t}$$

para todo x/t suficientemente grande para deducir, del ejercicio 27(b), que

$$\alpha + \frac{\beta}{2} + \frac{a}{2} + \frac{\varepsilon}{2} + \frac{a\varepsilon}{2} > 2a.$$

Puesto que ε es arbitrario esto implica

$$\alpha + \frac{\beta}{2} + \frac{a}{2} \geq 2a.$$

[Indicación: Hagamos que $x \rightarrow \infty$ de forma que $A(x)/x \rightarrow \alpha$.]

(b) Por medio de un argumento análogo, probar que

$$\beta + \frac{\alpha}{2} + \frac{a}{2} \leq 2a$$

y deducir que $\alpha = \beta = a$. Con otras palabras, $A(x) \sim ax$ cuando $x \rightarrow \infty$.

29. Tomar $a(n) = 1 + \mu(n)$ y comprobar que (52) se satisface con $a = 1$ y $b = 2C - 1$, en donde C es la constante de Euler. Probar que el resultado del ejercicio 28 implica

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \mu(n) = 0.$$

Esto nos proporciona otra demostración del teorema 4.14.

30. Suponemos que, en el ejercicio 28, no se admite el teorema del número primo. Admitiremos, en substitución,

$$\gamma = \liminf_{x \rightarrow \infty} \frac{\psi(x)}{x}, \quad \delta = \limsup_{x \rightarrow \infty} \frac{\psi(x)}{x}.$$

(a) Demostrar que la argumentación sugerida en el ejercicio 28 conduce a las desigualdades

$$\alpha + \frac{\beta}{2} + \frac{a\delta}{2} \geq 2a, \quad \beta + \frac{\alpha}{2} + \frac{a\gamma}{2} \leq 2a.$$

(b) De las desigualdades de la parte (a) probar que

$$a\gamma \leq \alpha \leq \beta \leq a\delta.$$

Este resultado prueba que los límites de indeterminación más ampliamente separados

$$\liminf_{x \rightarrow \infty} \frac{A(x)}{x} \quad \text{y} \quad \limsup_{x \rightarrow \infty} \frac{A(x)}{x},$$

se obtienen para $a(n) = a\Lambda(n)$, entre todos los números $a(n)$ que satisfacen (51) y (52) con a fijo. Por lo tanto para deducir $A(x) \sim ax$ de (51) y (52) basta tratar únicamente el caso especial $a(n) = a\Lambda(n)$.

Capítulo 5

Congruencias

5.1 DEFINICIÓN Y PROPIEDADES BÁSICAS DE LAS CONGRUENCIAS

Gauss introdujo una notación notable que simplifica muchos problemas relativos a la divisibilidad de los enteros. En este sentido creó una nueva rama de la Teoría de números llamada *teoría de congruencias*, cuyos fundamentos se discutirán en ese capítulo.

Salvo indicación expresa, las letras latinas y griegas minúsculas designarán enteros (positivos, negativos, o cero).

Definición. Dados enteros a, b, m con $m > 0$, decimos que a es congruente con b módulo m , y escribimos

$$(1) \quad a \equiv b \pmod{m},$$

si m divide la diferencia $a - b$. El número m se llama módulo de la congruencia.

En otras palabras, la congruencia (1) es equivalente a la relación de divisibilidad

$$m \mid (a - b).$$

En particular, $a \equiv 0 \pmod{m}$ si, y sólo si, $m \mid a$. Por lo tanto $a \equiv b \pmod{m}$ si, y sólo si, $a - b \equiv 0 \pmod{m}$. Si $m \nmid (a - b)$ escribimos $a \not\equiv b \pmod{m}$ y decimos que a y b son *incongruentes* mod m .

EJEMPLOS

1. $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $3^2 \equiv -1 \pmod{5}$.
2. n es par si, y sólo si, $n \equiv 0 \pmod{2}$.
3. n es impar si, y sólo si, $n \equiv 1 \pmod{2}$.
4. $a \equiv b \pmod{1}$ para cada a y b .
5. Si $a \equiv b \pmod{m}$ entonces $a \equiv b \pmod{d}$ cuando $d|m$, $d > 0$.

El símbolo de congruencia $\equiv$ fue elegido por Gauss para sugerir una analogía con el signo de igualdad $=$. Los dos teoremas que siguen prueban que las congruencias poseen de hecho muchas de las propiedades formales de las ecuaciones.

Teorema 5.1 *La congruencia es una relación de equivalencia. Esto es, tenemos:*

- | | |
|--|------------------|
| (a) $a \equiv a \pmod{m}$ | (reflexividad) |
| (b) $a \equiv b \pmod{m}$ implica $b \equiv a \pmod{m}$ | (simetría) |
| (c) $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$
implica $a \equiv c \pmod{m}$ | (transitividad). |

DEMOSTRACIÓN. La demostración sigue inmediatamente de las siguientes propiedades de divisibilidad:

- (a) $m|0$.
- (b) Si $m|(a - b)$ entonces $m|(b - a)$.
- (c) Si $m|(a - b)$ y $m|(b - c)$ entonces $m|(a - b) + (b - c) = m|a - c$. $\square$

Teorema 5.2 *Si $a \equiv b \pmod{m}$ y $\alpha \equiv \beta \pmod{m}$, entonces tenemos:*

- (a) $ax + \alpha y \equiv bx + \beta y \pmod{m}$ para todo entero x e y .
- (b) $a\alpha \equiv b\beta \pmod{m}$.
- (c) $a^n \equiv b^n \pmod{m}$ para cada entero positivo n .
- (d) $f(a) \equiv f(b) \pmod{m}$ para cada polinomio f con coeficientes enteros.

DEMOSTRACIÓN. (a) Dado que $m|(a - b)$ y $m|(\alpha - \beta)$ tenemos

$$m|x(a - b) + y(\alpha - \beta) = (ax + \alpha y) - (bx + \beta y).$$

- (b) Obsérvese que $a\alpha - b\beta = \alpha(a - b) + b(\alpha - \beta) \equiv 0 \pmod{m}$ por la parte (a).
- (c) Hacemos $\alpha = a$ y $\beta = b$ en la parte (b) y utilizamos inducción sobre n .
- (d) Utilizar la parte (c) e inducción sobre el grado de f . $\square$

El teorema 5.2 nos dice que dos congruencias respecto del mismo módulo se pueden sumar, restar o multiplicar, miembro a miembro, como si fuesen ecuaciones. El mismo resultado es verdadero para un número finito de congruencias respecto

del mismo módulo.

Antes de desarrollar más propiedades de las congruencias damos dos ejemplos que ilustran su utilidad.

EJEMPLO 1 Regla de divisibilidad por 9. Un entero $n > 0$ es divisible por 9 si, y sólo si, la suma de los dígitos de su expresión decimal es divisible por 9. Esta propiedad se demuestra con facilidad si se usan congruencias. Si los dígitos de n en su expresión decimal son $a_0, a_1, \dots, a_k$, entonces

$$n = a_0 + 10a_1 + 10^2a_2 + \dots + 10^ka_k.$$

Utilizando el teorema 5.2 tenemos, módulo 9,

$$10 \equiv 1, \quad 10^2 \equiv 1, \dots, \quad 10^k \equiv 1 \pmod{9}$$

o sea

$$n \equiv a_0 + a_1 + \dots + a_k \pmod{9}.$$

Obsérvese que todas estas congruencias son válidas también módulo 3, luego un número es divisible por 3 si, y sólo si, la suma de sus dígitos es divisible por 3.

EJEMPLO 2 Los números de Fermat $F_n = 2^{2^n} + 1$ ya fueron mencionados en la introducción histórica. Los cinco primeros son primos:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad \text{y } F_4 = 65\,537.$$

Ahora probaremos que F_5 es divisible por 641 sin calcular explícitamente F_5 . Para ello consideramos la sucesión de potencias 2^{2^n} módulo 641. Tenemos

$$2^2 = 4, \quad 2^4 = 16, \quad 2^8 = 256, \quad 2^{16} = 65\,536 \equiv 154 \pmod{641},$$

o sea

$$2^{32} \equiv (154)^2 = 23\,716 \equiv 640 \equiv -1 \pmod{641}.$$

Por consiguiente $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$, o sea F_5 es compuesto.

Volvemos ahora a las propiedades generales de las congruencias. En general no es posible simplificar factores comunes no nulos de ambos miembros de una congruencia aun cuando sea posible en las ecuaciones. Por ejemplo, los dos miembros de la congruencia

$$48 \equiv 18 \pmod{10}$$

son divisibles por 6, pero si simplificamos el factor común 6 obtenemos un resultado incorrecto, $8 \equiv 3 \pmod{10}$. El teorema que sigue prueba que un factor común se puede simplificar si el módulo es divisible por dicho factor.

Teorema 5.3 Si $c > 0$ entonces

$$a \equiv b \pmod{m} \text{ si, y sólo si, } ac \equiv bc \pmod{mc}.$$

DEMOSTRACIÓN. Tenemos $m|(b-a)$ si, y sólo si, $cm|c(b-a)$.

El teorema que sigue describe una regla de simplificar válida cuando el módulo no sea divisible por el factor común.

Teorema 5.4 Ley de simplificación. Si $ac \equiv bc \pmod{m}$ y si $d = (m, c)$, entonces

$$a \equiv b \pmod{\frac{m}{d}}.$$

En otras palabras, un factor común c se puede simplificar si el módulo se divide por $d = (m, c)$. En particular, un factor común que es primo con el módulo se puede simplificar siempre.

DEMOSTRACIÓN. Dado que $ac \equiv bc \pmod{m}$ tenemos

$$m|c(a-b) \text{ o sea } \frac{m}{d} \left| \frac{c}{d}(a-b) \right|.$$

Pero $(m/d, c/d) = 1$ y por lo tanto $m/d|(a-b)$. □

Teorema 5.5 Suponemos que $a \equiv b \pmod{m}$. Si $d|m$ y $d|a$, entonces $d|b$.

DEMOSTRACIÓN. Es suficiente suponer que $d > 0$. Si $d|m$ entonces $a \equiv b \pmod{m}$ implica $a \equiv b \pmod{d}$. Pero, si $d|a$, entonces $a \equiv 0 \pmod{d}$ por lo que $b \equiv 0 \pmod{d}$. □

Teorema 5.6 Si $a \equiv b \pmod{m}$ entonces $(a, m) = (b, m)$. Con otras palabras, los números que son congruentes módulo m tienen el mismo mcd con m .

DEMOSTRACIÓN. Sea $d = (a, m)$ y $e = (b, m)$. Entonces $d|m$ y $d|a$, luego $d|b$; por lo tanto $d|e$. Análogamente, $e|m$, $e|b$, luego $e|a$; por lo tanto $e|d$. Por consiguiente $d = e$. □

Teorema 5.7 Si $a \equiv b \pmod{m}$ y si $0 \leq |b-a| < m$, entonces $a = b$.

DEMOSTRACIÓN. Puesto que $m|(a-b)$ tenemos $m \leq |a-b|$ salvo si $a-b=0$. □

Teorema 5.8 Tenemos $a \equiv b \pmod{m}$ si, y sólo si, a y b tienen el mismo resto cuando se dividen por m .

DEMOSTRACIÓN. Escribimos $a = mq + s$, $b = mQ + R$, en donde $0 \leq r < m$ y $0 \leq R < m$. Entonces $a - b \equiv r - R \pmod{m}$ y $0 \leq |r - R| < m$. Ahora utilizamos el teorema 5.7. $\square$

Teorema 5.9 Si $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$ con $(m, n) = 1$, entonces $a \equiv b \pmod{mn}$.

DEMOSTRACIÓN. Puesto que m y n dividen a $a - b$ y $(m, n) = 1$ también mn divide a $a - b$. $\square$

5.2 CLASES DE RESTOS Y SISTEMAS COMPLETOS DE RESTOS¹

Definición. Consideremos un módulo fijo $m > 0$. Designemos por $\hat{a}$ el conjunto de todos los enteros x tales que $x \equiv a \pmod{m}$ y llamemos a $\hat{a}$ la clase de restos de a módulo m .

Entonces $\hat{a}$ consta de todos los enteros de la forma $a + mq$, $q = 0, \pm 1, \pm 2, \dots$

Las siguientes propiedades de las clases de restos son consecuencia fácil de esta definición.

Teorema 5.10 Para un módulo m dado tenemos:

- (a) $\hat{a} = \hat{b}$ si, y sólo si, $a \equiv b \pmod{m}$.
- (b) Dos enteros x e y pertenecen a la misma clase de restos si, y sólo si, $x \equiv y \pmod{m}$.
- (c) Las m clases de restos $\hat{1}, \hat{2}, \dots, \hat{m}$ son disjuntas y su unión es el conjunto de todos los enteros.

DEMOSTRACIÓN. Las partes (a) y (b) se siguen inmediatamente de la definición. Para probar (c) observamos que los números $0, 1, 2, \dots, m - 1$ son incongruentes módulo m (en virtud del teorema 5.7). Por lo tanto, por la parte (b), las clases de restos

$$\hat{0}, \hat{1}, \hat{2}, \dots, \hat{m-1}$$

son disjuntas. Pero cada entero x pertenece a una de estas clases exactamente puesto que $x = qm + r$ en donde $0 \leq r < m$, o sea $x \equiv r \pmod{m}$ y por lo tanto $x \in \hat{r}$. Dado que $\hat{0} = \hat{m}$ hemos demostrado (c). $\square$

¹ Los sistemas completos de restos se denominarán también «sistemas residuales completos». (N. del T.).

Definición. Un conjunto de m representantes, uno de cada una de las clases de restos $\hat{1}, \hat{2}, \dots, \hat{m}$ se llama sistema completo de restos módulo m .

EJEMPLOS Todo conjunto formado de m enteros, incongruentes mod m , es un sistema completo de restos mod m . Por ejemplo,

$$\begin{aligned} \{1, 2, \dots, m\}; \quad & \{0, 1, 2, \dots, m-1\}; \\ \{1, m+2, 2m+3, 3m+4, \dots, m^2\}. \end{aligned}$$

Teorema 5.11 Suponemos $(k, m) = 1$. Si $\{a_1, \dots, a_m\}$ es un sistema completo de restos módulo m , también lo es $\{ka_1, \dots, ka_m\}$.

DEMOSTRACIÓN. Si $ka_i \equiv ka_j \pmod{m}$ entonces $a_i \equiv a_j \pmod{m}$ ya que $(k, m) = 1$. Por consiguiente ningún par de elementos del conjunto $\{ka_1, \dots, ka_m\}$ es congruente módulo m . Puesto que en este conjunto existen m elementos, constituye un sistema completo de restos. $\square$

5.3 CONGRUENCIAS LINEALES

Las congruencias polinómicas se pueden estudiar con éxito de forma análoga a como se estudian en Álgebra las ecuaciones polinómicas. Aquí, sin embargo, tratamos con polinomios $f(x)$ con coeficientes enteros, por lo que los valores de estos polinomios serán enteros cuando x sea entero. Un entero x que satisfaga la congruencia polinómica

$$(2) \quad f(x) \equiv 0 \pmod{m}$$

se llama *solución* de la congruencia. Además, si $x \equiv y \pmod{m}$ entonces $f(x) \equiv f(y) \pmod{m}$ o sea que cada congruencia que tenga una solución tiene una infinidad. Por consiguiente, convenimos que las soluciones pertenecientes a la misma clase de restos no deben contarse como distintas. Y cuando hablamos del *número* de soluciones de una congruencia del tipo (2) nos referimos al número de soluciones *incongruentes*, esto es, al número de soluciones contenidas en el conjunto $\{1, 2, \dots, m\}$ o en algún otro sistema completo de restos módulo m . Por consiguiente cada congruencia polinómica módulo m tiene a lo sumo m soluciones.

EJEMPLO 1 La congruencia lineal $2x \equiv 3 \pmod{4}$ carece de solución, puesto que $2x - 3$ es impar para cada x y, por consiguiente, no puede ser divisible por 4.

EJEMPLO 2 La congruencia cuadrática $x^2 \equiv 1 \pmod{8}$ admite exactamente cuatro soluciones dadas por $x \equiv 1, 3, 5, 7 \pmod{8}$.

La teoría de las congruencias lineales quedará totalmente descrita mediante los tres teoremas que siguen.

Teorema 5.12 *Suponemos que $(a, m) = 1$. Entonces la congruencia lineal*

$$(3) \quad ax \equiv b \pmod{m}$$

tiene exactamente una solución.

DEMOSTRACIÓN. Es preciso verificar únicamente los números $1, 2, \dots, m$, ya que constituyen un sistema residual completo. Por consiguiente formamos los productos $a, 2a, \dots, ma$. Puesto que $(a, m) = 1$ estos números constituyen también un sistema residual completo. Por lo tanto, sólo uno de estos productos es congruente con b módulo m . Esto es, existe un único x que satisface (3). $\square$

Si bien el teorema 5.12 nos dice que la congruencia lineal (3) tiene una solución única si $(a, m) = 1$, no nos dice cómo determinar tal solución a excepción de comprobar todos los números de un sistema residual completo. Se conocen métodos más expeditivos para determinar la solución; algunos de ellos se discuten más adelante en este mismo capítulo.

Nota. Si $(a, m) = 1$ la única solución de la congruencia $ax \equiv 1 \pmod{m}$ se llama *inverso* de a módulo m . Si a' es el inverso de a , entonces ba' es la solución de (3).

Teorema 5.13 *Suponemos que $(a, m) = d$. Entonces la congruencia lineal*

$$(4) \quad ax \equiv b \pmod{m}$$

tiene solución si, y sólo si, $d|b$.

DEMOSTRACIÓN. Si existe una solución entonces $d|b$ puesto que $d|m$ y $d|a$. Recíprocamente, si $d|b$ la congruencia

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

tiene una solución puesto que $(a/d, m/d) = 1$, y esta solución es también una solución de (4). $\square$

Teorema 5.14 *Suponemos que $(a, m) = d$ y suponemos que $d|b$. Entonces la congruencia lineal*

$$(5) \quad ax \equiv b \pmod{m}$$

tiene exactamente d soluciones módulo m . Vienen dadas por

$$(6) \quad t, t + \frac{m}{d}, t + 2\frac{m}{d}, \dots, t + (d-1)\frac{m}{d},$$

en donde t es la solución única módulo m/d , de la congruencia lineal

$$(7) \quad \frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d} \right).$$

• DEMOSTRACIÓN. Cada solución de (7) es también una solución de (5). Recíprocamente, cada solución de (5) satisface (7). Luego los d números escritos en (6) son soluciones de (7) y, por lo tanto, de (5). Dos cualesquiera de ellos no son congruentes módulo m puesto que las relaciones

$$t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m}, \text{ con } 0 \leq r < d, 0 \leq s < d$$

implican

$$r\frac{m}{d} \equiv s\frac{m}{d} \pmod{m}, \quad \text{y por lo tanto } r \equiv s \pmod{d}.$$

Pero $0 \leq |r - s| < d$ luego $r = s$.

Falta demostrar que (5) no tiene más soluciones que las descritas en (6). Si y es una solución de (5) entonces $ay \equiv at \pmod{m}$ luego $y \equiv t \pmod{m/d}$. Por lo tanto $y = t + km/d$ para un cierto k . Pero $k \equiv r \pmod{d}$ para un r que verifica $0 \leq r < d$. Por consiguiente

$$k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m} \text{ luego } y \equiv t + r\frac{m}{d} \pmod{m}.$$

Por consiguiente y es congruente módulo m con uno de los números descritos en (6). Esto termina la demostración. $\square$

En el capítulo 1 hemos demostrado que el mcd de dos números a y b es una combinación lineal de a y de b . Podemos deducir el mismo resultado como consecuencia del teorema 5.14.

Teorema 5.15 Si $(a, b) = d$ existen enteros x e y tales que

$$(8) \quad ax + by = d.$$

DEMOSTRACIÓN. La congruencia lineal $ax \equiv d \pmod{b}$ tiene una solución.

Por lo tanto existe un entero y tal que $d - ax = by$. Esto nos da $ax + by = d$ tal como requeríamos. $\square$

Nota. Geométricamente, los pares (x, y) que satisfacen (8) son puntos reticulares que pertenecen a una línea recta. La coordenada x de cada uno de estos puntos es una solución de la congruencia $ax \equiv d \pmod{b}$.

5.4 SISTEMAS RESIDUALES REDUCIDOS Y EL TEOREMA DE EULER/FERMAT

Definición. Un sistema residual reducido módulo m es todo conjunto de $\varphi(m)$ enteros, incongruentes módulo m , cada uno de ellos primo con m .

Nota. $\varphi(m)$ es el valor para m de la indicatriz de Euler, introducida en el capítulo 2.

Teorema 5.16 Si $\{a_1, a_2, \dots, a_{\varphi(m)}\}$ es un sistema residual reducido módulo m y si $(k, m) = 1$, entonces $\{ka_1, ka_2, \dots, ka_{\varphi(m)}\}$ es también un sistema residual reducido módulo m .

DEMOSTRACIÓN. Ningún par de números ka_i es congruente módulo m . Además, puesto que $(a_i, m) = (k, m) = 1$, tenemos $(ka_i, m) = 1$ luego cada ka_i es primo con m . $\square$

Teorema 5.17 Teorema de Euler-Fermat. Suponemos que $(a, m) = 1$. Entonces tenemos

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

DEMOSTRACIÓN. Sea $\{b_1, b_2, \dots, b_{\varphi(m)}\}$ un sistema residual reducido módulo m . Entonces $\{ab_1, ab_2, \dots, ab_{\varphi(m)}\}$ es también un sistema residual reducido. Por lo tanto el producto de todos los enteros del primer conjunto es congruente con el producto de los del segundo conjunto. Por consiguiente

$$b_1 \cdots b_{\varphi(m)} \equiv a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \pmod{m}.$$

Cada b_i es primo con m por lo que se puede simplificar cada b_i obteniéndose el teorema. $\square$

Teorema 5.18 Si un primo p no divide a a , entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

DEMOSTRACIÓN. Es un corolario del teorema anterior puesto que $\varphi(p) = p - 1$. $\square$

Teorema 5.19 Teorema pequeño de Fermat. *Para cada entero a y cada primo p tenemos*

$$a^p \equiv a \pmod{p}.$$

DEMOSTRACIÓN. Si $p \nmid a$ es el teorema 5.18. Si $p|a$ entonces tanto a^p como a son congruentes con $0 \pmod{p}$. $\square$

El teorema de Euler-Fermat sirve para calcular las soluciones de una congruencia lineal.

Teorema 5.20 Si $(a, m) = 1$, la solución (única mod m) de la congruencia lineal (9)

$$ax \equiv b \pmod{m}$$

viene dada por

$$(10) \quad x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

DEMOSTRACIÓN. El número x dado por (10) satisface (9) en virtud del teorema de Euler-Fermat. La solución es única mod m puesto que $(a, m) = 1$. $\square$

EJEMPLO 1 Resolver la congruencia $5x \equiv 3 \pmod{24}$.

Solución

Puesto que $(5, 24) = 1$ existe una solución única. Utilizando (10) obtenemos

$$x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^7 \pmod{24}$$

puesto que $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4$. Módulo 24 tenemos $5^2 \equiv 1$, y

$$5^4 \equiv 5^6 \equiv 1, \quad 5^7 \equiv 5, \quad \text{luego } x \equiv 15 \pmod{24}.$$

EJEMPLO 2 Resolver la congruencia $25x \equiv 15 \pmod{120}$.

Solución

Puesto que $d = (25, 120) = 5$ y $d|15$, la congruencia admite exactamente cinco soluciones módulo 120. Para obtenerlas dividimos por 5 y resolvemos la congruencia $5x \equiv 3 \pmod{24}$. Utilizando el ejemplo 1 y el teorema 5.14 vemos que las cinco soluciones vienen dadas por $x = 15 + 24k$, $k = 0, 1, 2, 3, 4$, o

$$x \equiv 15, 39, 63, 87, 111 \pmod{120}.$$

5.5 CONGRUENCIAS POLINÓMICAS MÓDULO p .

TEOREMA DE LAGRANGE

El teorema fundamental del Álgebra establece que, para cada polinomio f de grado $n \geq 1$, la ecuación $f(x) = 0$ tiene n soluciones en el cuerpo de los números complejos. No existe un resultado directamente análogo a este teorema para congruencias polinómicas. Por ejemplo, vemos que ciertas congruencias lineales carecen de soluciones, algunas tienen exactamente una solución, y otras en cambio tienen más de una. Luego, incluso en este caso especial, no parece que exista relación simple entre el número de soluciones y el grado del polinomio. Sin embargo, para congruencias módulo *primo* tenemos el siguiente teorema de Lagrange.

Teorema 5.21 (Lagrange). *Dado un primo p , sea*

$$f(x) = c_0 + c_1x + \cdots + c_nx^n$$

un polinomio de grado n con coeficientes enteros tales que $c_n \not\equiv 0 \pmod{p}$. Entonces la congruencia polinómica

$$(11) \quad f(x) \equiv 0 \pmod{p}$$

tiene a lo sumo n soluciones.

Nota. Este resultado es falso para módulos compuestos. Por ejemplo, la congruencia cuadrática $x^2 \equiv 1 \pmod{8}$ tiene 4 soluciones.

DEMOSTRACIÓN. Usamos inducción sobre el grado n de f . Cuando $n = 1$ la congruencia es lineal:

$$c_1x + c_0 \equiv 0 \pmod{p}.$$

Puesto que $c_1 \not\equiv 0 \pmod{p}$ tenemos $(c_1, p) = 1$ y existe exactamente una solución. Entonces suponemos que el teorema es válido para polinomios de grado $n - 1$. Suponemos también que la congruencia (11) tiene $n + 1$ soluciones no congruentes módulo p ; es decir

$$x_0, x_1, \dots, x_n,$$

tales que $f(x_k) \equiv 0 \pmod{p}$ para cada $k = 0, 1, \dots, n$. Llegamos a contradicción. Tenemos la identidad algebraica

$$f(x) - f(x_0) = \sum_{r=1}^n c_r(x^r - x_0^r) = (x - x_0)g(x)$$

en donde $g(x)$ es un polinomio de grado $n - 1$ con coeficientes enteros y con coeficiente principal c_n . Entonces tenemos

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p},$$

puesto que $f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}$. Pero $x_k - x_0 \not\equiv 0 \pmod{p}$ si $k \neq 0$ luego, para cada $k \neq 0$, debe verificarse $g(x_k) \equiv 0 \pmod{p}$. Pero esto significa que la congruencia $g(x) \equiv 0 \pmod{p}$ tiene n soluciones incongruentes módulo p , en contradicción con nuestra hipótesis de inducción. Así termina la demostración. $\square$

5.6 APLICACIONES DEL TEOREMA DE LAGRANGE

Teorema 5.22 Si $f(x) = c_0 + c_1x + \dots + c_nx^n$ es un polinomio de grado n con coeficientes enteros y si la congruencia

$$f(x) \equiv 0 \pmod{p}$$

tiene más de n soluciones, en donde p es primo, entonces, cada coeficiente de f es divisible por p .

DEMOSTRACIÓN. Si existe algún coeficiente no divisible por p , sea c_k el que tiene mayor índice con esta propiedad. Entonces $k \leq n$ y la congruencia

$$c_0 + c_1x + \dots + c_kx^k \equiv 0 \pmod{p}$$

tiene más de k soluciones luego, por el teorema de Lagrange, $p|c_k$, contradicción. $\square$

Ahora aplicamos el teorema 5.22 a un polinomio particular.

Teorema 5.23 Para cada primo p todos los coeficientes del polinomio

$$f(x) = (x - 1)(x - 2) \cdots (x - p + 1) - x^{p-1} + 1$$

son divisibles por p .

DEMOSTRACIÓN. Sea $g(x) = (x - 1)(x - 2) \cdots (x - p + 1)$. Las raíces de g son los números $1, 2, \dots, p - 1$, puesto que satisfacen la congruencia

$$g(x) \equiv 0 \pmod{p}.$$

Por el teorema de Euler-Fermat, estos números satisfacen también la congruencia $h(x) \equiv 0 \pmod{p}$, donde

$$h(x) = x^{p-1} - 1.$$

La diferencia $f(x) = g(x) - h(x)$ tiene grado $p - 2$ pero la congruencia $f(x) \equiv 0 \pmod{p}$ tiene $p - 1$ soluciones, $1, 2, \dots, p - 1$. Por consiguiente, por el teorema 5.22, cada coeficiente de $f(x)$ es divisible por p . $\square$

Los dos teoremas que siguen se obtienen considerando dos coeficientes particulares del polinomio $f(x)$ del teorema 5.23.

Teorema 5.24 Teorema de Wilson. *Para todo primo p tenemos*

$$(p - 1)! \equiv -1 \pmod{p}.$$

DEMOSTRACIÓN. El término constante del polinomio $f(x)$ del teorema 5.23 es $(p - 1)! + 1$. $\square$

Nota. El recíproco del teorema de Wilson también se verifica. Esto es, si $n > 1$ y $(n - 1)! \equiv -1 \pmod{n}$, entonces n es primo. (Ver ejercicio 5.7.)

Teorema 5.15 Teorema de Wolstenholme. *Para todo primo $p \geq 5$ tenemos*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}.$$

DEMOSTRACIÓN. La suma en cuestión es la suma de los productos de los números $1, 2, \dots, p - 1$ tomando sólo $p - 2$ cada vez. Esta suma es también igual al coeficiente de $-x$ en el polinomio

$$g(x) = (x - 1)(x - 2) \cdots (x - p + 1).$$

En efecto, $g(x)$ se puede escribir en la forma

$$g(x) = x^{p-1} - S_1 x^{p-2} + S_2 x^{p-3} - \cdots + S_{p-3} x^2 - S_{p-2} x + (p - 1)!,$$

en donde el coeficiente S_k es la k -ésima función elemental simétrica de las raíces, esto es, la suma de los productos de los números $1, 2, \dots, p - 1$, tomados de k en k . El teorema 5.23 prueba que cada uno de los números $S_1, S_2, \dots, S_{p-2}$ es divisible por p . Pretendemos probar que S_{p-2} es divisible por p^2 .

El producto que define $g(x)$ prueba que $g(p) = (p - 1)!$ luego

$$(p - 1)! = p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3} p^2 - S_{p-2} p + (p - 1)!.$$

Simplificando $(p-1)!$ y reduciendo la ecuación mod p^3 obtenemos, puesto que $p > 5$,

$$pS_{p-2} \equiv 0 \pmod{p^3},$$

y por lo tanto $S_{p-2} \equiv 0 \pmod{p^2}$, como se pretendía. $\square$

5.7 CONGRUENCIAS LINEALES SIMULTÁNEAS. EL TEOREMA DEL RESTO CHINO

Un sistema de dos o más congruencias lineales no tiene necesariamente solución, aunque cada una de las congruencias individuales si tenga solución. Por ejemplo, no existe ningún x que satisfaga simultáneamente $x \equiv 1 \pmod{2}$ y $x \equiv 0 \pmod{4}$, a pesar de que cada una de ellas, separadamente, tiene solución. En este ejemplo, los módulos 2 y 4 no son primos entre sí. Ahora demostraremos que todo sistema de dos o más congruencias lineales que, separadamente, admiten solución única se puede resolver también simultáneamente si los módulos son dos a dos primos entre sí. Empezaremos con un caso especial.

Teorema 5.26 Teorema del resto chino. *Suponemos que $m_1, \dots, m_r$ son enteros positivos, primos entre sí, dos a dos:*

$$(m_i, m_k) = 1 \quad \text{si } i \neq k.$$

Sean $b_1, \dots, b_r$ enteros arbitrarios. Entonces el sistema de congruencias

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

posee exactamente una solución módulo el producto $m_1 \dots m_r$.

DEMOSTRACIÓN. Sea $M = m_1 \dots m_r$ y sea $M_k = M/m_k$. Entonces $(M_k, m_k) = 1$, por lo tanto cada M_k admite un inverso único M'_k módulo m_k . Sea ahora

$$x = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \dots + b_r M_r M'_r.$$

Consideremos cada uno de los términos de esta suma módulo m_k . Dado que $M_i \equiv 0 \pmod{m_k}$ si $i \neq k$ tenemos

$$x \equiv b_k M_k M'_k \equiv b_k \pmod{m_k}.$$

Por lo tanto x satisface cada una de las congruencias del sistema. Es fácil probar además que el sistema posee una única solución módulo M . En efecto, si x e y son dos soluciones del sistema tenemos $x \equiv y \pmod{m_k}$ para cada k y, puesto que los m_k son, dos a dos primos entre sí, tendremos también $x \equiv y \pmod{M}$. Esto termina la demostración. $\square$

La extensión que sigue se deduce ahora fácilmente.

Teorema 5.27 *Suponemos que $m_1, \dots, m_r$ son primos entre sí, dos a dos. Sean $b_1, \dots, b_r$ enteros arbitrarios y $a_1, \dots, a_r$ enteros tales que verifican*

$$(a_k, m_k) = 1 \quad \text{para } k = 1, 2, \dots, r.$$

Entonces el sistema lineal de congruencias

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

tiene exactamente una solución módulo $m_1, m_2 \dots m_r$.

DEMOSTRACIÓN. Si a'_k designa el inverso de a_k módulo m_k , que existe puesto que $(a_k, m_k) = 1$, la congruencia $a_k x \equiv b_k \pmod{m_k}$ es equivalente a la congruencia $x \equiv b_k a'_k \pmod{m_k}$. Ahora aplicamos el teorema 5.26. $\square$

5.8 APLICACIONES DEL TEOREMA DEL RESTO CHINO

La primera aplicación se refiere a congruencias polinómicas relativas a módulos compuestos.

Teorema 5.28 *Sea f un polinomio con coeficientes enteros positivos $m_1, m_2, \dots, m_r$ primos dos a dos, y $m = m_1 m_2 \dots m_r$. Entonces la congruencia*

$$(12) \quad f(x) \equiv 0 \pmod{m}$$

tiene una solución si, y sólo si, cada una de las congruencias

$$f(x) \equiv 0 \pmod{m_i} \quad (i = 1, 2, \dots, r)$$

admite una solución. Además, si $v(m)$ y $v(m_i)$ designan el número de soluciones de (12) y de (13), respectivamente, entonces

$$(14) \quad v(m) = v(m_1)v(m_2) \cdots v(m_r).$$

DEMOSTRACIÓN. Si $f(a) \equiv 0 \pmod{m}$ entonces $f(a) \equiv 0 \pmod{m_i}$ para cada i . Luego cada solución de (12) es también una solución de (13).

Recíprocamente, sea a_i una solución de (13). Entonces por el teorema del resto chino existe un entero a tal que

$$a \equiv a_i \pmod{m_i} \quad \text{para } i = 1, 2, \dots, r,$$

luego

$$f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}.$$

Puesto que los módulos son primos entre sí, dos a dos, tenemos también $f(a) \equiv 0 \pmod{m}$. Por consiguiente, si cada una de las congruencias de (13) tiene una solución, también la tiene (12).

Sabemos además por el teorema 5,26 que cada r -pla de soluciones $(a_1, \dots, a_r)$ de las congruencias de (13) proporciona un único entero $a \pmod{m}$ que satisface (15). Cada a_i recorre las $v(m_i)$ soluciones de (13), luego el número de enteros a que satisfacen (15) y, por ende, (13) es $v(m_1) \cdots v(m_r)$. Esto demuestra (14). $\square$

Nota. Si m admite la descomposición en factores primos

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

en el teorema 5,28 tomamos $m_i = p_i^{\alpha_i}$ y observamos que el problema de resolver una congruencia polinómica para un módulo compuesto se reduce a resolverla para módulos que son potencias de primos. Más adelante demostraremos que el problema se puede reducir en última instancia a congruencias polinómicas relativas a módulos primos más un conjunto de congruencias lineales. (Ver sección 5.9.)

La aplicación del teorema del resto chino que sigue se refiere a los puntos reticulares visibles desde el origen. (Ver sección 3.8.)

Teorema 5.29 *El conjunto de puntos reticulares del plano visibles desde el origen contiene vacíos cuadrados tan grandes como queramos. Esto es, dado un entero $k > 0$ existe un punto reticular (a, b) tal que ninguno de los puntos reticulares*

$$(a + r, b + s), \quad 0 < r \leq k, 0 < s \leq k,$$

es visible desde el origen.

DEMOSTRACIÓN. Sea $p_1, p_2, \dots$, la sucesión de primos. Dado $k > 0$ consideramos la matriz $k \times k$ que en su primera fila contiene los k primeros números primos, en su segunda fila los k siguientes y así sucesivamente. Sea m_i el producto de los primos de la i -ésima fila y sea M_i el producto de los primos de la i -ésima columna. Entonces los números m_i son primos entre sí, dos a dos, así como los M_i .

Ahora consideremos el conjunto de congruencias

$$\begin{aligned} x &\equiv -1 \pmod{m_1} \\ x &\equiv -2 \pmod{m_2} \\ &\vdots \\ x &\equiv -k \pmod{m_k}. \end{aligned}$$

Este sistema tiene una solución a que es única mod $m_1 \dots m_k$. Análogamente, el sistema

$$\begin{aligned} y &\equiv -1 \pmod{M_1} \\ &\vdots \\ y &\equiv -k \pmod{M_k} \end{aligned}$$

tiene una solución b que es única mod $M_1 \dots M_k = m_1 \dots m_k$.

Ahora consideremos el cuadrado cuyos vértices opuestos son (a, b) y $(a + k, b + k)$. Todo punto reticular del interior de este cuadrado es de la forma

$$(a + r, b + s), \quad \text{en donde } 0 < r < k, 0 < s < k,$$

y los puntos con $r = k$ o $s = k$ pertenecen a la frontera del cuadrado. Ahora probaremos que ninguno de estos puntos es visible desde el origen. En efecto,

$$a \equiv -r \pmod{m_r} \quad \text{y} \quad b \equiv -s \pmod{M_s}$$

luego el número primo que se halla en la intersección de la fila r y la columna s divide a $a + r$ y a $b + s$. Por lo tanto $a + r$ y $b + s$ no son primos entre sí, y por consiguiente el punto reticular $(a + r, b + s)$ no es visible desde el origen. $\square$

5.9 CONGRUENCIAS POLINÓMICAS RELATIVAS A POTENCIAS DE PRIMOS

El teorema 5.28 muestra que el problema de resolver una congruencia polinómica

$$f(x) \equiv 0 \pmod{m}$$

se puede reducir al problema de resolver un sistema de congruencias

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \quad (i = 1, 2, \dots, r),$$

en donde $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. En esta sección veremos que el problema se puede reducir en última instancia a congruencias relativas a módulos primos más un cierto conjunto de congruencias lineales.

Sea f un polinomio con coeficientes enteros, y supongamos que para un cierto número primo p y un cierto $\alpha \geq 2$ la congruencia

$$(16) \quad f(x) \equiv 0 \pmod{p^\alpha}$$

tiene una solución $x = a$, en donde a se ha elegido de forma que pertenezca al intervalo

$$0 \leq a < p^\alpha.$$

Esta solución satisface además cada una de las congruencias $f(x) \equiv 0 \pmod{p^\beta}$ para cada $\beta < \alpha$. En particular, a satisface la congruencia

$$(17) \quad f(x) \equiv 0 \pmod{p^{\alpha-1}}.$$

Ahora dividimos a por $p^{\alpha-1}$ y escribimos

$$(18) \quad a = qp^{\alpha-1} + r, \text{ donde } 0 \leq r < p^{\alpha-1}.$$

Se dice que el resto r determinado por (18) ha sido *generado* por a . Dado que $r \equiv a \pmod{p^{\alpha-1}}$, el número r es también una solución de (17). Con otras palabras, cada solución a de la congruencia (16) perteneciente al intervalo $0 \leq a < p^\alpha$ genera una solución r de la congruencia (17) en el intervalo $0 \leq r < p^{\alpha-1}$.

Partimos ahora de una solución r de (17) perteneciente al intervalo $0 \leq r < p^{\alpha-1}$ y nos preguntamos cuando existirá una solución a de (16) que pertenezca al intervalo $0 \leq a < p^\alpha$ que genere r . Cuando ocurra, diremos que r se puede *subir* de

p^{a-1} a p^a . El teorema que sigue demuestra que la posibilidad de que r pueda subirse depende de $f(r) \bmod p^a$ y de la derivada $f'(r) \bmod p$.

Teorema 5.30 *Suponemos que $\alpha \geq 2$ y que r es una solución de la congruencia*

$$(19) \quad f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

que pertenece al intervalo $0 \leq r < p^{\alpha-1}$.

(a) *Suponemos que $f'(r) \not\equiv 0 \pmod{p}$. Entonces r puede subirse de forma única de p^{a-1} a p^a . Esto es, existe un único a en el intervalo $0 \leq a < p^a$ que genera r y que satisface la congruencia*

$$(20) \quad f(x) \equiv 0 \pmod{p^a}.$$

(b) *Suponemos $f'(r) \equiv 0 \pmod{p}$. Entonces tenemos dos posibilidades:*

(b₁) *Si $f(r) \equiv 0 \pmod{p^a}$, r puede subirse de p^{a-1} a p^a de p formas distintas.*

(b₂) *Si $f(r) \not\equiv 0 \pmod{p^a}$, r no puede subirse de p^{a-1} a p^a .*

DEMOSTRACIÓN. Si n es el grado de f tenemos la identidad (fórmula de Taylor)

$$(21) \quad f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n$$

para cada x y h . Observemos que cada polinomio $f^{(k)}(x)/k!$ tiene coeficientes enteros. (El lector puede comprobar esta afirmación.) Ahora hacemos $x = r$ en (21), en donde r es una solución de (19) perteneciente al intervalo $0 \leq r < p^{\alpha-1}$, y sea $h = qp^{\alpha-1}$ en donde q es un entero que a continuación especificaremos. Dado que $\alpha \geq 2$, los términos de (21) que contienen h^2 y potencias superiores de h son múltiplos enteros de p^a . Por consiguiente (21) nos da la congruencia

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^a}.$$

Puesto que r satisface (19) podemos escribir $f(r) = kp^{\alpha-1}$ para algún entero k , y la última congruencia nos conduce a

$$f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1} \pmod{p^a}.$$

Sea ahora

$$(22) \quad a = r + qp^{\alpha-1}.$$

Entonces a satisface la congruencia (20) si, y sólo si, q satisface la congruencia lineal

$$(23) \quad qf'(r) + k \equiv 0 \pmod{p}.$$

Si $f'(r) \not\equiv 0 \pmod{p}$ esta congruencia tiene una solución única $q \pmod{p}$, y si elegimos q en el intervalo $0 \leq q < p$ entonces el número a dado por (22) satisfará (20) y pertenecerá al intervalo $0 \leq a < p^a$.

Por otro lado, si $f'(r) \equiv 0 \pmod{p}$ entonces (23) tiene una solución q si, y sólo si, $p|k$, esto es, si y sólo si $f(r) \equiv 0 \pmod{p^a}$. Si $p \nmid k$ no existe ninguna elección de q tal que a satisfaga (20). Pero, si $p|k$, entonces los p valores $q = 0, 1, \dots, p-1$ dan p soluciones a de (20) que generan r y pertenecen al intervalo $0 \leq a < p^a$. Esto termina la demostración. $\square$

La demostración del teorema anterior describe también un método para obtener soluciones de la congruencia (20), si se conocen soluciones de (19). Aplicando repetidamente el método el problema queda reducido en última instancia a resolver la congruencia

$$(24) \quad f(x) \equiv 0 \pmod{p}.$$

Si (24) carece de soluciones, entonces (20) carece de soluciones. Si (24) tiene soluciones, elegimos una, llamémosla r , que pertenezca al intervalo $0 \leq r < p$. En correspondencia con r existirán 0, 1 ó p soluciones de la congruencia

$$(25) \quad f(x) \equiv 0 \pmod{p^2}$$

dependiendo de los números $f'(r)$ y $k = f(r)/p$. Si $p \nmid k$ y $p|f'(r)$, entonces r no puede subirse a una solución de (25). En este caso empezamos de nuevo con una solución diferente r . Si ninguna r puede subirse, entonces (25) carece de solución.

Si $p|k$ para algún r , examinamos la congruencia lineal

$$qf'(r) + k \equiv 0 \pmod{p}.$$

Esta ecuación admite 1 ó p soluciones q según que $p \nmid f'(r)$ o que $p|f'(r)$. Para cada solución q , el número $a = r + qp$ da una solución de (25). Para cada una de las soluciones de (25), podemos utilizar un procedimiento análogo para obtener todas las soluciones de

$$f(x) \equiv 0 \pmod{p^3},$$

y así sucesivamente, hasta obtener todas las soluciones de (20).

5.10 EL PRINCIPIO DE LA CLASIFICACIÓN CRUZADA

Algunos problemas de Teoría de números se pueden tratar aplicando un teorema combinatorio general relativo a conjuntos, llamado el *principio de la clasificación cruzada*. Es una fórmula que cuenta el número de elementos de un conjunto finito S que no pertenecen a ciertos subconjuntos prescritos $S_1, \dots, S_n$.

Notación. Si T es un subconjunto de S escribiremos $N(T)$ para designar el número de elementos de T . Designaremos por $S - T$ al conjunto de elementos de S que no pertenecen a T . Entonces

$$S - \bigcup_{i=1}^n S_i$$

consta de los elementos de S que no pertenecen a ninguno de los subconjuntos $S_1, \dots, S_n$. Por brevedad escribiremos $S_i S_j$, $S_i S_j S_k$, ..., para designar las intersecciones $S_i \cap S_j$, $S_i \cap S_j \cap S_k$, ..., respectivamente.

Teorema 5.31 Principio de la clasificación cruzada. Si $S_1, \dots, S_n$ son subconjuntos dados de un conjunto finito S , entonces

$$\begin{aligned} N\left(S - \bigcup_{i=1}^n S_i\right) &= N(S) - \sum_{1 \leq i \leq n} N(S_i) + \sum_{1 \leq i < j \leq n} N(S_i S_j) \\ &\quad - \sum_{1 \leq i < j < k \leq n} N(S_i S_j S_k) + \cdots + (-1)^n N(S_1 S_2 \cdots S_n). \end{aligned}$$

DEMOSTRACIÓN. Si $T \subseteq S$, $N_r(T)$ designa el número de elementos de T que no pertenecen a ninguno de los r primeros subconjuntos $S_1, \dots, S_r$, y siendo $N_0(T)$ simplemente $N(T)$. Los elementos contados por $N_{r-1}(T)$ pertenecen a dos conjuntos disjuntos, el conjunto de los que no pertenecen a S_r y el de los que pertenecen a S_r . Por consiguiente tenemos

$$N_{r-1}(T) = N_r(T) + N_{r-1}(TS_r).$$

Luego

$$(26) \quad N_r(T) = N_{r-1}(T) - N_{r-1}(TS_r).$$

Hagamos ahora $T = S$ y usemos (26) para expresar cada término del segundo miembro de N_{r-2} . Obtenemos

$$\begin{aligned} N_r(S) &= \{N_{r-2}(S) - N_{r-2}(SS_{r-1})\} - \{N_{r-2}(S_r) - N_{r-2}(S_r S_{r-1})\} \\ &= N_{r-2}(S) - N_{r-2}(S_{r-1}) - N_{r-2}(S_r) + N_{r-2}(S_r S_{r-1}). \end{aligned}$$

Aplicando repetidamente (26) obtenemos finalmente

$$N_r(S) = N_0(S) - \sum_{i=1}^r N_0(S_i) + \sum_{1 \leq i < j \leq r} N_0(S_i S_j) - \cdots + (-1)^r N_0(S_1 \cdots S_r).$$

Cuando $r = n$ esto nos proporciona la fórmula requerida. $\square$

EJEMPLO La fórmula producto para la indicatriz de Euler se puede obtener del principio de la clasificación cruzada. Si $p_1, \dots, p_r$ designan los divisores primos de n , sean $S = \{1, 2, \dots, n\}$ y S_k el subconjunto de S formado por los enteros divisibles por p_k . Los números de S primos con n son los que no pertenecen a ninguno de los conjuntos $S_1, \dots, S_r$, luego

$$\varphi(n) = N\left(S - \bigcup_{k=1}^r S_k\right).$$

Si $d|n$ existen n/d múltiplos de d que pertenecen al conjunto S . Luego

$$N(S_i) = \frac{n}{p_i}, N(S_i S_j) = \frac{n}{p_i p_j}, \dots, N(S_1 \cdots S_r) = \frac{n}{p_1 \cdots p_r},$$

por lo tanto el principio de la clasificación cruzada nos da

$$\begin{aligned} \varphi(n) &= n - \sum_{i=1}^r \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\ &= n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

La aplicación del principio de la clasificación cruzada que sigue cuenta el número de elementos de un sistema residual reducido módulo k que pertenecen a una clase de restos $r \bmod d$, en donde $d|k$ y $(r, d) = 1$.

Teorema 5.32 *Dados enteros r, d y k tales que $d|k$, $d > 0$, $k \geq 1$ y $(r, d) = 1$, el número de elementos del conjunto*

$$S = \{r + td : t = 1, 2, \dots, k/d\}$$

que son primos con k es $\varphi(k)/\varphi(d)$.

DEMOSTRACIÓN. Si un primo p divide a k y a $r + td$, entonces $p \nmid d$, ya que en caso contrario $p \mid r$, contradiciendo la hipótesis $(r, d) = 1$. Por consiguiente, los primos que dividen a k y a los elementos de S son los que dividen a k pero no dividen a d . Llamemóslas $p_1, \dots, p_m$ y sea

$$k' = p_1 p_2 \cdots p_m.$$

Entonces los elementos de S primos con k son los que no son divisibles por ninguno de estos primos. Sea

$$S_i = \{x : x \in S \text{ y } p_i \nmid x\} \quad (i = 1, 2, \dots, m).$$

Si $x \in S_i$ y $x = r + td$, entonces $r + td \equiv 0 \pmod{p_i}$. Como $p_i \nmid d$ existe un único $t \pmod{p_i}$ con esta propiedad, y por consiguiente exactamente un t en cada uno de los intervalos $[1, p_i], [p_i + 1, 2p_i], \dots, [(q-1)p_i + 1, qp_i]$ en donde $qp_i = k/d$.

Por consiguiente

$$N(S_i) = \frac{k/d}{p_i}.$$

Análogamente,

$$N(S_i S_j) = \frac{k/d}{p_i p_j}, \dots, N(S_1 \cdots S_m) = \frac{k/d}{p_1 \cdots p_m}.$$

Luego por el principio de la clasificación cruzada el número de enteros de S que son primos con k es

$$N\left(S - \bigcup_{i=1}^m S_i\right) = \frac{k}{d} \sum_{\delta \mid k'} \frac{\mu(\delta)}{\delta} = \frac{k}{d} \prod_{p \mid k'} \left(1 - \frac{1}{p}\right) = \frac{k \prod_{p \mid k} \left(1 - \frac{1}{p}\right)}{d \prod_{p \mid d} \left(1 - \frac{1}{p}\right)} = \frac{\varphi(k)}{\varphi(d)}. \quad \square$$

5.11 UNA PROPIEDAD DE DESCOMPOSICIÓN DE LOS SISTEMA RESIDUALES REDUCIDOS

Como aplicación del teorema anterior analizamos una propiedad de los sistemas residuales reducidos que utilizaremos en un capítulo posterior. Empezamos con un ejemplo numérico.

Sea S un sistema residual reducido mod 15, por ejemplo

$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Disponemos los 8 elementos de S en una matriz 4×2 como sigue:

$$\begin{bmatrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{bmatrix}.$$

Obsérvese que cada fila contiene un sistema residual reducido mod 3, y los números de cada columna son congruentes entre sí mod 3. Este ejemplo ilustra una propiedad general de los sistemas residuales reducidos descrito en el teorema que sigue.

Teorema 5.33 *Sea S un sistema residual reducido mod k , y sea $d > 0$ un divisor de k . Entonces tenemos las siguientes descomposiciones de S :*

(a) S es la reunión de $\varphi(k)/\varphi(d)$ conjuntos disjuntos, cada uno de los cuales es un sistema residual reducido mod d .

(b) S es la reunión de $\varphi(d)$ conjuntos disjuntos, cada uno de los cuales consta de $\varphi(k)/\varphi(d)$ números congruentes entre sí mod d .

Nota. En el ejemplo anterior, $k = 15$ y $d = 3$. Las filas de la matriz representan los conjuntos disjuntos de la parte (a), y las columnas representan los conjuntos disjuntos de la parte (b). Si aplicamos el teorema al divisor $d = 5$, obtenemos la descomposición dada por la matriz

$$\begin{bmatrix} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{bmatrix}.$$

Cada fila es un sistema residual reducido mod 5 y cada columna consta de números congruentes entre sí mod. 5.

DEMOSTRACIÓN. En primer lugar demostraremos que las partes (a) y (b) son equivalentes. Si (b) se verifica podemos disponer los $\varphi(k)$ elementos de S en forma de matriz, utilizando para ello los $\varphi(d)$ conjuntos disjuntos de (b) como columnas. Esta matriz tiene $\varphi(k)/\varphi(d)$ filas. Cada fila contiene un sistema reducido mod d , y estos son los conjuntos disjuntos requeridos en la parte (a). Análogamente, es fácil comprobar que (a) implica (b).

Ahora probaremos (b). Sea S_d un sistema residual reducido mod d , y sea $r \in S_d$. Probaremos que existen por lo menos $\varphi(k)/\varphi(d)$ enteros n en S , distintos mod k , tales que $n \equiv r \pmod{d}$. Puesto que existen $\varphi(d)$ valores de r en S_d y $\varphi(k)$ enteros en S , no pueden existir más de $\varphi(k)/\varphi(d)$ de tales números n , lo cual demuestra la parte (b).

Los números n requeridos se seleccionan en las clases de restos mod k representadas por los k/d enteros siguientes:

$$r, r + d, r + 2d, \dots, r + \frac{k}{d}d.$$

Estos números son congruentes entre sí mod d y entre sí son incongruentes mod k . Puesto que $(r, d) = 1$, el teorema 5.32 prueba que $\varphi(k)/\varphi(d)$ de ellos son primos con k , lo que termina la demostración. (Para una demostración diferente basada en la teoría de grupos ver [1]). $\square$

Ejercicios del capítulo 5 5

1. Sea S un conjunto de n enteros (no necesariamente distintos). Probar que algún subconjunto no vacío de S posee una suma divisible por n .
2. Probar que $5n^3 + 7n^5 \equiv 0 \pmod{12}$ para todo entero n .
3. (a) Hallar todos los enteros positivos n tales que $n^{13} \equiv n \pmod{1365}$.
(b) Hallar todos los enteros positivos n tales que $n^{17} \equiv n \pmod{4080}$.
4. (a) Probar que $\varphi(n) \equiv 2 \pmod{4}$ cuando $n = 4$ y cuando $n = p^a$, en donde p es un primo, $p \equiv 3 \pmod{4}$.
(b) Hallar todos los n tales que $\varphi(n) \equiv 2 \pmod{4}$.
5. Una regla dividida en 36 pulgadas se divide de nuevo en 70 partes iguales. Probar que entre las cuatro divisiones más pequeñas hay dos a las que corresponden las pulgadas 1 y 19 como extremos izquierdos. ¿Cuáles son los extremos derechos que corresponden a las otras dos?
6. Hallar todos los x que verifican simultáneamente el sistema de congruencias

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{4}, \quad x \equiv 3 \pmod{5}.$$

7. Probar el recíproco del teorema de Wilson: Si $(n-1)! + 1 \equiv 0 \pmod{n}$, entonces n es primo si $n > 1$.
8. Hallar todos los enteros n positivos para los que $(n-1)! + 1$ es una potencia de n .
9. Si p es un primo impar, sea $q = (p-1)/2$. Probar que

$$(q!)^2 + (-1)^q \equiv 0 \pmod{p}.$$

Esto nos proporciona $q!$ como solución explícita de la congruencia $x^2 + 1 \equiv 0 \pmod{p}$ cuando $p \equiv 1 \pmod{4}$, y demuestra que $q! \equiv \pm 1 \pmod{p}$ si $p \equiv 3 \pmod{4}$. No se conoce ninguna regla general simple para determinar el signo.

10. Si p es impar, $p > 1$, probar que

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

y

$$2^2 4^2 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

11. Sea p un primo, $p \geq 5$, y hagamos

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{r}{ps}.$$

Probar que $p^3 | (r-s)$.

12. Si p es un primo, probar que

$$\binom{n}{p} \equiv \left[\frac{n}{p} \right] \pmod{p}.$$

Luego, si $p^a | [n_0 p]$ probar que

$$p^a | \binom{n}{p}.$$

13. Sean a, b, n enteros positivos tales que n divide a $a^n - b^n$. Probar que n divide también a $(a^n - b^n)/(a - b)$.
14. Sean a, b y x_0 enteros positivos y definamos

$$x_n = ax_{n-1} + b \quad \text{para } n = 1, 2, \dots$$

Probar que no es posible que todos los x_n sean primos.

15. Sean n, r, a enteros positivos. La congruencia $n^2 \equiv n \pmod{10^a}$ implica $n^r \equiv n \pmod{10^a}$ para todo r . Hallar todos los valores de r tales que $n^r \equiv n \pmod{10^a}$ implica $n^2 \equiv n \pmod{10^a}$.
16. Sean n, a, d enteros con $(a, d) = 1$. Probar que existe un entero m tal que $m \equiv a \pmod{d}$ y $(m, n) = 1$.
17. Sea f una función aritmética con valores enteros tal que

$$f(m+n) \equiv f(n) \pmod{m}$$

para todo $m \geq 1, n \geq 1$. Sea $g(n)$ el número de valores (contando las repeticiones) de $f(1), f(2), \dots, f(n)$ divisibles por n , y sea $h(n)$ el número de estos valores primos con n . Probar que

$$h(n) = n \sum_{d|n} \mu(d) \frac{g(d)}{d}.$$

18. Dado un entero impar $n > 3$, sean k y t los menores enteros positivos tales que tanto $kn + 1$ como tn son cuadrados. Probar que n es primo si, y sólo si, k y t son ambos mayores que $n/4$.
19. Probar que cada elemento del conjunto de los $n-1$ enteros consecutivos

$$n! + 2, n! + 3, \dots, n! + n$$

es divisible por un primo que no divide a ningún otro elemento del conjunto.

20. Probar que para todos los enteros positivos n y k , existe un conjunto de n enteros consecutivos tal que cada uno de los elementos de este conjunto es divisible por k primos distintos ninguno de los cuales divide a los otros elementos del conjunto.
21. Sea n un entero positivo que no es un cuadrado. Probar que, para cada entero a primo con n , existen enteros x e y que verifican

$$ax \equiv y \pmod{n} \quad \text{con} \quad 0 < x < \sqrt{n} \quad \text{y} \quad 0 < |y| < \sqrt{n}.$$

22. Sea un primo, $p \equiv 1 \pmod{4}$, sea $q = (p-1)/2$, y sea $a = g^q$
- (a) Probar que existen enteros positivos x e y que verifican $0 < x < \sqrt{p}$ y $0 < y < \sqrt{p}$ tales que

$$a^2x^2 - y^2 \equiv 0 \pmod{p}.$$

- (b) Probar que los x e y de la parte (a) verifican $p = x^2 + y^2$. Esto prueba que cada primo $p \equiv 1 \pmod{4}$ es la suma de dos cuadrados.
- (c) Probar que ningún primo $p \equiv 3 \pmod{4}$ es la suma de dos cuadrados.

Capítulo 6

Grupos abelianos finitos y sus caracteres

6.1 DEFINICIONES

En el capítulo 2 tuvimos ocasión de mencionar los grupos pero no hicimos uso esencial de sus propiedades. Ahora deseamos tratar con más detalle algunos aspectos elementales de la Teoría de grupos. El tratamiento del teorema de Dirichlet acerca de los primos en progresiones aritméticas que daremos en el capítulo 7 requerirá el conocimiento de ciertas funciones aritméticas llamadas *caracteres de Dirichlet*. Aunque el estudio de los caracteres de Dirichlet se puede acometer sin poseer ningún conocimiento de los grupos, la introducción de un mínimo de conocimientos sobre Teoría de grupos coloca la teoría de los caracteres de Dirichlet en un ámbito más general y simplifica el tratamiento.

Definición. Axiomas de grupo. Un grupo G es un conjunto no vacío provisto de una operación binaria, que designaremos por $\cdot$, que verifica los siguientes axiomas:

- (a) *Cerrada.* Para cada a y b de G , $a \cdot b$ también pertenece a G .
- (b) *Asociatividad.* Para cada a, b, c de G , tenemos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (c) *Existencia de identidad.* Existe un único elemento e en G , llamado identidad, tal que $a \cdot e = e \cdot a = a$ para cada a de G .
- (d) *Existencia de inversos.* Para cada a de G existe un único elemento b de G tal que $a \cdot b = b \cdot a = e$. Este b se designa a^{-1} y se llama el inverso de a .

Nota. Usualmente omitiremos el punto y escribiremos ab para indicar $a \cdot b$.

Definición. Grupo abeliano. Un grupo G se llama abeliano si cada par de elementos conmuta; esto es, si $ab = ba$ para todo a y b de G .

Definición. Grupo finito. Un grupo G es finito si G es un conjunto finito. En este caso el número de elementos de G se llama orden de G y se designa por $|G|$.

Definición. Subgrupo. Un subconjunto no vacío G' de un grupo G que, a su vez, sea un grupo respecto de la misma operación, se llama subgrupo de G .

6.2 EJEMPLOS DE GRUPOS Y SUBGRUPOS

EJEMPLO 1 Subgrupos triviales. Cada grupo G tiene por lo menos dos subgrupos: el mismo grupo G y el conjunto $\{e\}$ formado únicamente por el elemento identidad.

EJEMPLO 2 Enteros con la suma. El conjunto de todos los enteros es un grupo abeliano con la operación $+$ y 0 su elemento identidad. El inverso de n es $-n$.

EJEMPLO 3 Números complejos con la multiplicación. El conjunto de todos los números complejos no nulos es un grupo abeliano tomando como operación la multiplicación ordinaria de los números complejos, y como identidad el 1. El inverso de z es $1/z$. El conjunto de los números complejos de valor absoluto 1 es un subgrupo.

EJEMPLO 4 Las raíces n -ésimas de la unidad. Los grupos de los ejemplos 2 y 3 son grupos infinitos. Un ejemplo de grupo finito es el conjunto $\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$, en donde $\varepsilon = e^{2\pi i/n}$ y la operación $\cdot$ es la multiplicación usual de los números complejos. Este grupo, de orden n , se llama el grupo de las raíces n -ésimas de la unidad. Es un subgrupo de los dos grupos del ejemplo 3.

6.3 PROPIEDADES ELEMENTALES DE LOS GRUPOS

Los teoremas elementales que siguen se refieren a un grupo arbitrario G . Con otras palabras, no se impone que G sea abeliano, ni finito.

Teorema 6.1 Regla de simplificación. Si los elementos a, b, c de G satisfacen

$$ac = bc \quad \text{o} \quad ca = cb,$$

entonces $a = b$.

DEMOSTRACIÓN. En el primer caso multiplicamos cada miembro por la derecha

por c^{-1} y utilizamos la asociatividad. En el segundo caso multiplicamos por la izquierda por c^{-1} . $\square$

Teorema 6.2 Propiedades de los inversos. En todo grupo G tenemos:

- (a) $e^{-1} = e$.
- (c) Para cada a de G , $(a^{-1})^{-1} = a$.
- (c) Para todo a y b de G , $(ab)^{-1} = b^{-1}a^{-1}$. (Obsérvese que se invierte el orden.)
- (d) Para todo a y b de G la ecuación $ax = b$ admite la solución única $x = a^{-1}b$; la ecuación $ya = b$ admite la solución única $y = ba^{-1}$.

DEMOSTRACIÓN.

- (a) Puesto que $ee = ee^{-1}$ simplificamos e y tenemos $e = e^{-1}$.
- (b) Puesto que $aa^{-1} = e$ y los inversos son únicos, a es el inverso de a^{-1} .
- (c) Por la ley asociativa tenemos

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

luego $b^{-1}a^{-1}$ es el inverso de ab .

- (d) De nuevo por la asociatividad tenemos

$$a(a^{-1}b) = (aa^{-1})b = b \quad \text{y} \quad (ba^{-1})a = b(a^{-1}a) = b.$$

Las soluciones son únicas en virtud de la regla de simplificación. $\square$

Definición. Potencias de un elemento. Si $a \in G$ definimos a^n para todo entero n mediante las siguientes relaciones:

$$a^0 = e, \quad a^n = aa^{n-1}, \quad a^{-n} = (a^{-1})^n \quad \text{para } n > 0.$$

Las reglas de exponentes que siguen se pueden demostrar por inducción. Omitimos las demostraciones.

Teorema 6.3 Si $a \in G$, dos potencias cualesquiera de a conmutan, y para todo entero m y n tenemos

$$a^m a^n = a^{m+n} = a^n a^m \quad \text{y} \quad (a^m)^n = a^{mn} = (a^n)^m.$$

Además, si a y b conmutan tenemos

$$a^n b^n = (ab)^n.$$

Teorema 6.4 Criterio del subgrupo. Si G' es un subconjunto no vacío de un grupo G , entonces G' es un subgrupo si, y sólo si, G' satisface los axiomas (a) y (d) de los grupos:

(a) Cerrado: si $a, b \in G'$, entonces $ab \in G'$.

(d) Existencia de inverso: si $a \in G'$, entonces $a^{-1} \in G'$.

DEMOSTRACIÓN. Cada subgrupo G' posee ciertamente estas propiedades. Recíprocamente, si G' satisface (a) y (d) es fácil probar que G' también satisface los axiomas (b) y (c). El axioma (b), la asociatividad, se verifica en G' puesto que se verifica para todos los elementos de G . Para probar que (c) se verifica en G' observemos que existe un elemento a de G' (puesto que G' es no vacío) cuyo inverso $a^{-1} \in G'$ (por (d)) por lo que $aa^{-1} \in G'$ por (a). Pero $aa^{-1} = e$ luego $e \in G'$. $\square$

6.4 CONSTRUCCIÓN DE SUBGRUPOS

Podemos construir siempre un subgrupo de un grupo dado G eligiendo un elemento a cualquiera de G y formando el conjunto de todas sus potencias a^n , $n = 0, \pm 1, \pm 2, \dots$. Este conjunto satisface claramente los axiomas (a) y (d), luego es un subgrupo de G . Se llama *subgrupo cíclico engendrado* por a y se designa por $\langle a \rangle$.

Obsérvese que $\langle a \rangle$ es abeliano aunque G no lo sea. Si $a^n = e$ para algún entero positivo n , existirá un $n > 0$ mínimo con esta propiedad y el subgrupo $\langle a \rangle$ será un grupo finito de orden n ,

$$\langle a \rangle = \{a, a^2, \dots, a^{n-1}, a^n = e\}.$$

El entero n se llama también *orden del elemento* a . Un ejemplo de subgrupo cíclico de orden n lo constituye el grupo de las raíces n -ésimas de la unidad mencionado en la sección 6.2.

El próximo teorema prueba que cada elemento de un grupo finito tiene orden finito.

Teorema 6.5 Si G es finito y $a \in G$, entonces existe un entero positivo $n \leq |G|$ tal que $a^n = e$.

DEMOSTRACIÓN. Sea $g = |G|$. Entonces, por lo menos, dos de los $g + 1$ elementos de G siguientes, han de ser iguales:

$$e, a, a^2, \dots, a^g.$$

Si suponemos que $a^r = a^s$, en donde $0 \leq s < r \leq g$, tenemos

$$e = a^r(a^s)^{-1} = a^{r-s}.$$

Esto demuestra el teorema con $n = r - s$. □

Como hemos observado en la sección 6.2, cada grupo G posee dos subgrupos triviales, $\{e\}$ y el propio G . Cuando G es un grupo abeliano finito existe un procedimiento simple para construir una colección creciente de subgrupos intermedios entre $\{e\}$ y G . Este procedimiento, que describiremos en el teorema 6.8, se basa en la siguiente observación.

Si G' es un subgrupo de un grupo finito G , entonces para cada elemento a de G existe un entero n tal que $a^n \in G'$. Si a pertenece ya a G' tomamos simplemente $n = 1$. Si $a \notin G'$ tomamos n igual al orden de a , puesto que $a^n = e \in G'$. Sin embargo, puede existir una potencia positiva de a menor que pertenezca a G' . Por el principio de buena ordenación existe un entero positivo mínimo n tal que $a^n \in G'$. A este entero lo llamaremos *indicador* de a en G' .

Teorema 6.6 *Sea G' un subgrupo de un grupo finito abeliano G , con $G' \neq G$. Elegimos un elemento a de G , $a \notin G'$, y sea h el indicador de a en G' . Entonces el conjunto de los productos*

$$G'' = \{xa^k : x \in G' \text{ y } k = 0, 1, 2, \dots, h-1\}$$

es un subgrupo de G que contiene a G' . Además el orden de G'' es h veces el de G' ,

$$|G''| = h|G'|.$$

DEMOSTRACIÓN. Para probar que G'' es un subgrupo utilizamos el criterio del subgrupo. Veamos que es cerrado. Elegimos dos elementos de G'' , por ejemplo xa^k e ya^j , con $x, y \in G'$ y $0 \leq k < h$, $0 \leq j < h$. Puesto que G es abeliano el producto de los elementos es

$$(1) \quad (xy)a^{k+j}.$$

Sea ahora $k+j = qh + r$ en donde $0 \leq r < h$. Entonces

$$a^{k+j} = a^{qh+r} = a^{qh}a^r = za^r,$$

en donde $z = a^{qh} = (a^h)^q \in G'$ puesto que $a^h \in G'$. Por consiguiente el elemento de (1) es $(xyz)a^r = wa^r$, en donde $w \in G'$ y $0 \leq r < h$. Esto demuestra que G'' es cerrado.

Ahora probaremos que el inverso de cada elemento de G'' también está en G'' . Elegimos un elemento arbitrario de G'' , xa^k . Si $k = 0$ entonces el inverso es x^{-1} que pertenece a G' . Si $0 < k < h$, el inverso es el elemento

$$ya^{h-k}, \text{ en donde } y = x^{-1}(a^h)^{-1},$$

que de nuevo pertenece a G'' . Esto prueba que G'' también es efectivamente un subgrupo de G . Es claro que G'' contiene a G' .

Ahora determinaremos el orden de G'' . Sea $m = |G'|$. Cuando x recorre los m elementos de G' y k recorre los h enteros $0, 1, 2, \dots, h-1$ obtenemos mh productos xa^k . Si probamos que todos ellos son *distintos*, entonces G'' tiene orden mh . Consideremos dos de estos productos, por ejemplo xa^k e ya^j y suponemos que

$$xa^k = ya^j \text{ con } 0 \leq j \leq k < h.$$

Entonces $a^{k-j} = x^{-1}y$ y $0 \leq k-j < h$. Puesto que $x^{-1}y \in G'$ el elemento a^{k-j} pertenecerá a G' , luego $k=j$ y por lo tanto $x=y$. Esto termina la demostración. $\square$

6.5 CARACTERES DE GRUPOS ABELIANOS FINITOS

Definición. Sea G un grupo arbitrario. Una función f con valores complejos definida en G se llama un carácter de G si f tiene la propiedad multiplicativa

$$f(ab) = f(a)f(b)$$

para todo a, b de G , y si $f(c) \neq 0$ para algún c de G .

Teorema 6.7 Si f es un carácter de un grupo finito G con elemento identidad e , entonces $f(e) = 1$ y cada valor $f(a)$ de la función es una raíz de la unidad. Efectivamente, si $a^n = e$ entonces $f(a)^n = 1$.

DEMOSTRACIÓN. Elegimos c en G de forma que $f(c) \neq 0$. Puesto que $ce = c$ tenemos

$$f(c)f(e) = f(c)$$

luego $f(e) = 1$. Si $a^n = e$ entonces $f(a)^n = f(a^n) = f(e) = 1$. $\square$

EJEMPLO Cada grupo G admite un carácter por lo menos, que es la función idénticamente igual a 1 en G . Se llama carácter *principal*. El teorema que sigue nos dice que, si G es abeliano y tiene orden finito > 1 , admite otros caracteres.

Teorema 6.8 Un grupo abeliano G finito de orden n admite exactamente n caracteres distintos.

DEMOSTRACIÓN. En el teorema 6.6 hemos aprendido a construir a partir de un subgrupo $G' \neq G$, un nuevo subgrupo G'' que contiene a G' y que posee por lo menos un elemento a más que G' . Utilizaremos el símbolo $\langle G'; a \rangle$ para designar el subgrupo G'' construido en el teorema 6.6. Entonces

$$\langle G'; a \rangle = \{xa^k : x \in G' \text{ y } 0 \leq k < h\}$$

en donde h es el indicador de a en G' .

Ahora aplicamos esta construcción repetidamente, partiendo del subgrupo $\{e\}$ que designamos por G_1 . Si $G_1 \neq G$, sea a_1 un elemento de G distinto de e y definamos $G_2 = \langle G_1; a_1 \rangle$. Si $G_2 \neq G$, sea a_2 un elemento de G que no esté en G_2 y definamos $G_3 = \langle G_2; a_2 \rangle$. Continuemos este proceso a fin de obtener un conjunto finito de elementos $a_1, a_2, \dots, a_t$ y un conjunto asociado de subgrupos $G_1, G_2, \dots, G_{t+1}$ tales que

$$G_{r+1} = \langle G_r; a_r \rangle$$

con

$$G_1 \subset G_2 \subset \dots \subset G_{t+1} = G.$$

El proceso debe acabar con un número finito de pasos ya que el grupo dado G es finito y cada G_{r+1} contiene más elementos que su predecesor G_r . Considerando esta cadena de subgrupos demostramos el teorema por inducción, viendo que, si es cierto para G_r , también lo es para G_{r+1} .

Es claro que para G_1 sólo existe un carácter, que es la función que es idénticamente 1. Supongamos, ahora, que G_r tiene orden m y que existen exactamente m caracteres distintos para G_r . Consideramos $G_{r+1} = \langle G_r; a_r \rangle$ y sea h el indicador de a_r en G_r , esto es, el menor entero positivo tal que $a_r^h \in G_r$. Probaremos que existen exactamente h maneras diferentes de extender cada carácter de G_r para obtener un carácter de G_{r+1} , y que cada carácter de G_{r+1} es la extensión de algún carácter de G_r . Esto probará que G_{r+1} tiene exactamente mh caracteres, y puesto que mh es también el orden de G_{r+1} habremos demostrado el teorema por inducción sobre r .

Un elemento típico de G_{r+1} tiene la forma

$$xa_r^k, \text{ en donde } x \in G_r \text{ y } 0 \leq k < h.$$

De momento suponemos que es posible extender un carácter f de G_r a G_{r+1} . Llamemos $\tilde{f}$ a esta extensión y veamos qué puede decirse acerca de $\tilde{f}(xa_r^k)$. La propiedad multiplicativa requiere

$$\tilde{f}(xa_r^k) = \tilde{f}(x)\tilde{f}(a_r)^k.$$

Pero $x \in G_r$, luego $\tilde{f}(x) = f(x)$ y la ecuación anterior implica

$$\tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r)^k.$$

Esto nos dice que $\tilde{f}(xa_r^k)$ está determinado si se conoce $\tilde{f}(a_r)$.

¿Qué valores son posibles para $\tilde{f}(a_r)$? Sea $c = a_r^h$. Dado que $c \in G_r$, tenemos $\tilde{f}(c) = f(c)$, y puesto que $\tilde{f}$ es multiplicativo tenemos además $\tilde{f}(c) = \tilde{f}(a_r)^h$. Entonces

$$\tilde{f}(a_r)^h = f(c),$$

luego $\tilde{f}(a_r)$ es una de las h -ésimas raíces de $f(c)$. Por lo tanto existen a lo sumo h elecciones posibles para $\tilde{f}(a_r)$.

Estas observaciones nos indican cómo se puede definir $\tilde{f}$. Si f es un carácter dado de G_r , elegimos una de las h -ésimas raíces de $f(c)$, en donde $c = a_r^h$, y definimos $\tilde{f}(a_r)$ igual a dicha raíz. Entonces definimos $\tilde{f}$ en el resto de G_{r+1} por medio de la ecuación

$$(2) \quad \tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r)^k.$$

Las h elecciones posibles para $\tilde{f}(a_r)$ son todas diferentes, lo que nos da h formas diferentes de definir $\tilde{f}(xa_r^k)$. Ahora comprobaremos que la función $\tilde{f}$ definida de esta forma tiene la propiedad multiplicativa requerida. De (2) obtenemos

$$\begin{aligned} \tilde{f}(xa_r^k \cdot ya_r^j) &= \tilde{f}(xy \cdot a_r^{k+j}) = f(xy)\tilde{f}(a_r)^{k+j} \\ &= f(x)f(y)\tilde{f}(a_r)^k\tilde{f}(a_r)^j \\ &= \tilde{f}(xa_r^k)\tilde{f}(ya_r^j), \end{aligned}$$

luego $\tilde{f}$ es un carácter de G_{r+1} . Dos extensiones $\tilde{f}$ y $\tilde{g}$ no pueden ser idénticas sobre G_{r+1} puesto que las funciones f y g que extienden tendrían que ser idénticas en G_r . Por consiguiente cada uno de los m caracteres de G_r se puede extender de h formas diferentes a fin de producir un carácter de G_{r+1} . Además, si φ es un carácter arbitrario de G_{r+1} entonces su restricción a G_r también es un carácter de G_r , luego el proceso de extensión produce todos los caracteres de G_{r+1} . Esto termina la demostración. $\square$

6.6 EL GRUPO DE LOS CARACTERES

En esta sección G es un grupo finito abeliano de orden n . El carácter principal de G se designa f_1 . Los restantes, designados $f_2, f_3, \dots, f_n$, se llaman caracteres no principales, y tienen la propiedad: $f(a) \neq 1$ para algún a de G .

Teorema 6.9 Si definimos la multiplicación de caracteres por medio de la relación

$$(f_i f_j)(a) = f_i(a) f_j(a)$$

para cada a de G , entonces el conjunto de caracteres de G forma un grupo abeliano de orden n . Este grupo lo designamos $\hat{G}$. El elemento identidad de $\hat{G}$ es el carácter principal f_1 . El inverso de f_i es $1/f_i$.

DEMOSTRACIÓN. La comprobación de los axiomas de grupo es un ejercicio fácil y se omiten los detalles.

Nota. Para cada carácter f tenemos $|f(a)| = 1$. Luego el inverso $1/f(a)$ es igual al complejo conjugado $\overline{f(a)}$. Por lo tanto la función $\bar{f}$ definida por $\bar{f}(a) = \overline{f(a)}$ también es un carácter de G . Además tenemos, para cada a de G ,

$$\bar{f}(a) = \frac{1}{f(a)} = f(a^{-1}).$$

6.7 RELACIONES DE ORTOGONALIDAD PARA CARACTERES

Sea G un grupo abeliano finito de orden n , de elementos $a_1, a_2, \dots, a_n$, y sean $f_1, f_2, \dots, f_n$ los caracteres de G en donde f_1 es el carácter principal.

Notación. Designamos $A = A(G)$ la matriz $n \times n$ cuyo elemento a_{ij} de la i -ésima fila j -ésima columna es

$$a_{ij} = f_i(a_j).$$

Probaremos que la matriz A tiene inversa y utilizaremos este hecho para deducir las llamadas relaciones de ortogonalidad para caracteres. Primero determinaremos la suma de los elementos de cada fila de A .

Teorema 6.10 La suma de los elementos de la i -ésima fila de A viene dada por

$$\sum_{r=1}^n f_i(a_r) = \begin{cases} n & \text{si } f_i \text{ es el carácter principal } (i = 1), \\ 0 & \text{en otro caso.} \end{cases}$$

DEMOSTRACIÓN. S designa la suma en cuestión. Si $f_i = f_1$ cada término de la

suma es 1 y $S = n$. Si $f_i \neq f_j$, existe un elemento b de G tal que $f_i(b) \neq 1$. Cuando a_r recorre los elementos de G , lo mismo ocurre con los productos ba_r . Luego

$$S = \sum_{r=1}^n f_i(ba_r) = f_i(b) \sum_{r=1}^n f_i(a_r) = f_i(b)S.$$

Por consiguiente $S(1 - f_i(b)) = 0$. Puesto que $f_i(b) \neq 1$ obtenemos que $S = 0$. $\square$

Utilizaremos ahora este resultado para demostrar que A tiene inversa.

Teorema 6.11 *Sea A^* la matriz conjugada traspuesta de la matriz A . Entonces tenemos*

$$AA^* = nI,$$

en donde I es la matriz identidad $n \times n$. Luego $n^{-1}A^*$ es la inversa de A .

DEMOSTRACIÓN. Sea $B = AA^*$. El elemento b_{ij} perteneciente a la i -ésima fila j -ésima columna de B viene dado por

$$b_{ij} = \sum_{r=1}^n f_i(a_r)\bar{f}_j(a_r) = \sum_{r=1}^n (f_i\bar{f}_j)(a_r) = \sum_{r=1}^n f_k(a_r),$$

en donde $f_k = f_i\bar{f}_j = f_i/f_j$. Ahora bien $f_i/f_j = f_1$ si, y sólo si, $i = j$. Luego por el teorema 6.10 tenemos

$$b_{ij} = \begin{cases} n & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Con otras palabras, $B = nI$. $\square$

Ahora utilizamos el hecho de que una matriz conmuta con su inversa para obtener las relaciones de ortogonalidad para caracteres.

Teorema 6.12 *Relaciones de ortogonalidad para caracteres. Tenemos*

$$(3) \quad \sum_{r=1}^n \bar{f}_r(a_i)f_r(a_j) = \begin{cases} n & \text{si } a_i = a_j, \\ 0 & \text{si } a_i \neq a_j. \end{cases}$$

DEMOSTRACIÓN. La relación $AA^* = nI$ implica $A^*A = nI$. Pero el elemento de la i -ésima fila y j -ésima columna de A^*A es la suma de la izquierda de (3). Esto termina la demostración. $\square$

Nota. Puesto que $\bar{f}(a_i) = f_r(a_i)^{-1} = f_r(a_i^{-1})$, el término general de la suma de (3) es igual a $f_r(a_i^{-1})f_r(a_j) = f_r(a_i^{-1}a_j)$. Por consiguiente las relaciones de ortogonalidad se pueden expresar como sigue:

$$\sum_{r=1}^n f_r(a_i^{-1}a_j) = \begin{cases} n & \text{si } a_i = a_j, \\ 0 & \text{si } a_i \neq a_j. \end{cases}$$

Cuando a_i es el elemento identidad e obtenemos:

Teorema 6.13 *La suma de los elementos de la j -ésima columna de A se obtiene por*

$$(4) \quad \sum_{r=1}^n f_r(a_j) = \begin{cases} n & \text{si } a_j = e, \\ 0 & \text{en otro caso.} \end{cases}$$

6.8 CARACTERES DE DIRICHLET

La exposición anterior se refería a caracteres de un grupo abeliano finito arbitrario G . Ahora imponemos que G sea el grupo de las clases reducidas de restos módulo un entero positivo fijo k . En primer lugar probaremos que estas clases de restos forman, ciertamente, un grupo si definimos de manera conveniente la multiplicación.

Recordemos que un sistema residual reducido módulo k es un conjunto de $\varphi(k)$ enteros $\{a_1, a_2, \dots, a_{\varphi(k)}\}$ incongruentes módulo k , cada uno de ellos primo con k . Para cada entero a la clase de restos correspondientes $\hat{a}$ es el conjunto de todos los enteros congruentes con a módulo k :

$$\hat{a} = \{x: x \equiv a \pmod{k}\}.$$

La multiplicación de las clases de restos se define por la relación

$$(5) \quad \hat{a} \cdot \hat{b} = \widehat{ab}.$$

Esto es, el producto de dos clases de restos $\hat{a}$ y $\hat{b}$ es la clase de restos del producto ab .

Teorema 6.14 *Con la multiplicación definida en (5), el conjunto de clases reducidas de restos, módulo k , es un grupo finito y abeliano de orden $\varphi(k)$. El elemento unidad es la clase de restos $\hat{1}$. El inverso de $\hat{a}$ es la clase de restos $\hat{b}$, en donde $ab \equiv 1 \pmod{k}$.*

DEMOSTRACIÓN. La operación es cerrada: se satisface automáticamente en

virtud de la forma en que se ha definido la multiplicación de clases de restos. La clase $\hat{1}$ es claramente el elemento identidad. Si $(a, k) = 1$ existe un único b tal que $ab \equiv 1 \pmod{k}$. Luego el inverso de $\hat{a}$ es $\hat{b}$. Finalmente es claro que el grupo es abeliano y que es de orden $\varphi(k)$. $\square$

Definición. Caracteres de Dirichlet. Sea G el grupo de clases reducidas de restos módulo k . En correspondencia con cada carácter f de G definimos una función aritmética $\chi = \chi_f$ como sigue:

$$\begin{aligned}\chi(n) &= f(\hat{n}) & \text{si } (n, k) = 1, \\ \chi(n) &= 0 & \text{si } (n, k) > 1.\end{aligned}$$

La función χ se llama un carácter de Dirichlet módulo k . El carácter principal χ_1 es el que verifica las propiedades

$$\chi_1(n) = \begin{cases} 1 & \text{si } (n, k) = 1, \\ 0 & \text{si } (n, k) > 1. \end{cases}$$

Teorema 6.15 *Existen $\varphi(k)$ caracteres de Dirichlet módulo k , cada uno de los cuales es completamente multiplicativo y periódico de período k . Es decir, se verifica*

$$\begin{aligned}(6) \quad & \chi(mn) = \chi(m)\chi(n) \quad \text{para todo } m, n \\ & \chi(n+k) = \chi(n) \quad \text{para todo } n.\end{aligned}$$

Recíprocamente, si χ es completamente multiplicativo y periódico de período k , y si $\chi(n) = 0$ si $(n, k) > 1$, entonces χ es uno de los caracteres de Dirichlet módulo k .

DEMOSTRACIÓN. Existen $\varphi(k)$ caracteres f para el grupo G de las clases reducidas de restos módulo k , luego $\varphi(k)$ caracteres χ_f módulo k . La propiedad multiplicativa (6) de χ_f se sigue de la de f cuando m y n son primos con k . Si uno de ellos, m o n , no es primo con k entonces tampoco lo es mn , luego los dos miembros de (6) son cero. La propiedad de la periodicidad se sigue del hecho de que $\chi_f(n) = f(\hat{n})$ y de que $a \equiv b \pmod{k}$ implica $(a, k) = (b, k)$.

Para probar el recíproco observamos que la función f definida en el grupo G por la ecuación

$$f(\hat{n}) = \chi(n) \quad \text{si } (n, k) = 1$$

es un carácter de G , o sea χ es un carácter de Dirichlet mod k . $\square$

EJEMPLO Cuando $k = 1$ o $k = 2$, entonces $\varphi(k) = 1$ y el único carácter de Dirichlet es el carácter principal χ_1 . Para $k \geq 3$, existen, por lo menos, dos carac-

terres puesto que $\varphi(k) \geq 2$. Las tablas que siguen muestran todos los caracteres de Dirichlet para $k = 3, 4$ y 5 .

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0
$k = 3, \varphi(k) = 2$			

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0
$k = 4, \varphi(k) = 2$				

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0
$k = 5, \varphi(k) = 4$					

Para rellenar estas tablas utilizamos que $\chi(n)^{\varphi(k)} = 1$ siempre que $(n, k) = 1$, luego $\chi(n)$ es una $\varphi(k)$ -ésima raíz de la unidad. Observamos además que, si χ es un carácter módulo k , su conjugado $\bar{\chi}$ también lo es. Esta información es suficiente para completar las tablas para $k = 3$ y $k = 4$.

Cuando $k = 5$ tenemos $\varphi(5) = 4$, luego los posibles valores de $\chi(n)$ son ± 1 y $\pm i$ cuando $(n, 5) = 1$. Además, $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$, luego $\chi(2)$ y $\chi(3)$ son inversos. Puesto que $\chi(4) = \chi(2)^2$ esta información es suficiente para rellenar la tabla en el caso $k = 5$. Como comprobación podemos utilizar los teoremas 6.10 y 6.13 que nos dicen que la suma de los elementos de cada fila y de cada columna es cero salvo para la primera. Las tablas que siguen describen los caracteres de Dirichlet mod 6 y 7.

n	1	2	3	4	5	6
$\chi_1(n)$	1	0	0	0	1	0
$\chi_2(n)$	1	0	0	0	-1	0
$k = 6, \varphi(k) = 2$						

n	1	2	3	4	5	6	7
$\chi_1(n)$	1	1	1	1	1	1	0
$\chi_2(n)$	1	1	-1	1	-1	-1	0
$\chi_3(n)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_4(n)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_5(n)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_6(n)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0
$k = 7, \varphi(k) = 6$							

En nuestro estudio del teorema de Dirichlet relativo a los primos de una progresión aritmética haremos uso de la siguiente relación de ortogonalidad relativa a caracteres módulo k .

Teorema 6.16 Sean $\chi_1, \dots, \chi_{\varphi(k)}$ los $\varphi(k)$ caracteres de Dirichlet módulo k . Sean m y n dos enteros, con $(n, k) = 1$. Entonces tenemos

$$\sum_{r=1}^{\varphi(k)} \chi_r(m) \bar{\chi}_r(n) = \begin{cases} \varphi(k) & \text{si } m \equiv n \pmod{k}. \\ 0 & \text{si } m \not\equiv n \pmod{k}, \end{cases}$$

DEMOSTRACIÓN. Si $(m, k) = 1$, tomamos $a_i = \hat{n}$ y $a_j = \hat{m}$ en las relaciones de ortogonalidad del teorema 6.12 y observamos que $\hat{m} = \hat{n}$ si, y sólo si, $m \equiv n \pmod{k}$. Si $(m, k) > 1$ cada término de la suma se anula y $m \not\equiv n \pmod{k}$. $\square$

6.9 SUMAS QUE CONTIENEN CARACTERES DE DIRICHLET

Esta sección discute ciertas sumas que aparecen en la demostración del teorema de Dirichlet relativo a primos en progresiones aritméticas.

El primer teorema se refiere a un carácter no principal $\chi \pmod{k}$, pero la demostración es válida si χ es una función aritmética periódica con período k y que tiene sumas parciales acotadas.

Teorema 6.17 *Sea χ un carácter no principal módulo k , y sea f una función no negativa que, para todo $x \geq x_0$, admite derivada continua no negativa $f'(x)$. Entonces, si $y \geq x \geq x_0$, tenemos*

$$(7) \quad \sum_{x < n \leq y} \chi(n) f(n) = O(f(x)).$$

Si, además, $f(x) \rightarrow 0$ cuando $x \rightarrow \infty$, entonces la serie infinita

$$\sum_{n=1}^{\infty} \chi(n) f(n)$$

converge y tenemos, para $x \geq x_0$,

$$(8) \quad \sum_{n \leq x} \chi(n) f(n) = \sum_{n=1}^{\infty} \chi(n) f(n) + O(f(x)).$$

DEMOSTRACIÓN. Sea $A(x) = \sum_{n \geq x} \chi(n)$. Puesto que χ no es principal tenemos

$$A(k) = \sum_{n=1}^k \chi(n) = 0.$$

Por la periodicidad obtenemos que $A(nk) = 0$ para $n = 2, 3, \dots$, luego $|A(x)| < \varphi(k)$ para todo x . Con otras palabras, $A(x) = O(1)$.

Ahora utilizamos la identidad de Abel (teorema 4.2) para expresar la suma de (7) en forma de integral, lo que nos proporciona

$$\begin{aligned}\sum_{x < n \leq y} \chi(n)f(n) &= f(y)A(y) - f(x)A(x) - \int_x^y A(t)f'(t) dt \\ &= O(f(y)) + O(f(x)) + O\left(\int_x^y (-f'(t)) dt\right) = O(f(x)).\end{aligned}$$

Esto demuestra (7). Si $f(x) \rightarrow 0$ cuando $x \rightarrow \infty$, entonces (7) prueba que la serie

$$\sum_{n=1}^{\infty} \chi(n)f(n)$$

converge en virtud del criterio de convergencia de Cauchy. Para probar (8) basta observar simplemente que

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n \leq x} \chi(n)f(n) + \lim_{y \rightarrow \infty} \sum_{x < n \leq y} \chi(n)f(n).$$

En virtud de (7) el límite de la derecha es $O(f(x))$. Ello termina la demostración. $\square$

Ahora aplicamos el teorema 6.17 sucesivamente con $f(x) = 1/x$, $f(x) = (\log x)/x$, y $f(x) = 1/\sqrt{x}$ para $x \geq 1$ para obtener:

Teorema 6.18 Si χ es un carácter no principal mod k y si $x \geq 1$ tenemos

$$(9) \quad \sum_{n \leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right),$$

$$(10) \quad \sum_{n \leq x} \frac{\chi(n) \log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n} + O\left(\frac{\log x}{x}\right),$$

$$(11) \quad \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right).$$

6.10 LA NO ANULACIÓN DE $L(1, \chi)$ PARA χ NO PRINCIPAL REAL

Designamos por $L(1, \chi)$ a la suma de la serie de (9). Así,

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

En la demostración del teorema de Dirichlet necesitamos saber que $L(1, \chi) \neq 0$ cuando χ es un carácter no principal. Aquí demostraremos este resultado para caracteres no principales reales. Ante todo consideraremos la suma de divisores de $\chi(n)$.

Teorema 6.19 Sea χ un carácter real mod k y sea

$$A(n) = \sum_{d|n} \chi(d).$$

Entonces $A(n) \geq 0$ para todo n , y $A(n) \geq 1$ si n es un cuadrado.

DEMOSTRACIÓN. Para potencias de primos tenemos

$$A(p^a) = \sum_{i=0}^a \chi(p^i) = 1 + \sum_{i=1}^a \chi(p)^i.$$

Dado que χ es real los únicos valores posibles de $\chi(p)$ son 0, 1 y -1 . Si $\chi(p) = 0$ entonces $A(p^a) = 1$; si $\chi(p) = 1$, entonces $A(p^a) = a + 1$ y si $\chi(p) = -1$ entonces

$$A(p^a) = \begin{cases} 0 & \text{si } a \text{ impar,} \\ 1 & \text{si } a \text{ es par.} \end{cases}$$

En todo caso, $A(p^a) \geq 1$ si a es par.

Ahora si $n = p_1^{a_1} \dots p_r^{a_r}$, entonces $A(n) = A(p_1^{a_1}) \dots A(p_r^{a_r})$ puesto que A es multiplicativa. Cada factor $A(p_i^{a_i}) \geq 0$ luego $A(n) \geq 0$. Además, si n es un cuadrado, entonces cada exponente a_i es par, luego cada factor $A(p_i^{a_i}) \geq 1$; por lo tanto $A(n) \geq 1$. Esto demuestra el teorema. $\square$

Teorema 6.20 Para todo carácter no principal real χ mod k , sea

$$A(n) = \sum_{d|n} \chi(d) \quad \text{y} \quad B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

Entonces tenemos:

- (a) $B(x) \rightarrow \infty$ cuando $x \rightarrow \infty$.
- (b) $B(x) = 2\sqrt{x}L(1, \chi) + O(1)$ para todo $x \geq 1$.

Por consiguiente $L(1, \chi) \neq 0$.

DEMOSTRACIÓN. Para demostrar la parte (a) utilizamos el teorema 6.19 para escribir

$$B(x) \geq \sum_{\substack{n \leq x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

La última suma tiende a ∞ cuando $x \rightarrow \infty$ puesto que la serie armónica $\sum 1/m$ diverge.

Para probar la parte (b) escribimos

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q, d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

Ahora invocamos el teorema 3.17 que establece que

$$\sum_{\substack{q, d \\ qd \leq x}} f(d)g(q) = \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b)$$

en donde $ab = x$, $F(x) = \sum_{n \leq x} f(n)$, y $G(x) = \sum_{n \leq x} g(n)$. Tomamos $a = b = \sqrt{x}$ y hacemos $f(n) = \chi(n)/\sqrt{n}$, $g(n) = 1/\sqrt{n}$ para obtener

$$(12) \quad B(x) = \sum_{\substack{q, d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}).$$

Por el teorema 3.2 tenemos

$$G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right)$$

en donde A es una constante, y por el teorema 6.18, ecuación (11), tenemos

$$F(x) = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right),$$

en donde $B = \sum_{n=1}^{\infty} \chi(n)/\sqrt{n}$. Puesto que $F(\sqrt{x})G(\sqrt{x}) = 2Bx^{1/4} + O(1)$, la ecuación (12) nos da

$$B(x) = \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left\{ 2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right) \right\} +$$

$$\begin{aligned}
& + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} \left\{ B + O\left(\sqrt{\frac{n}{x}}\right) \right\} - 2Bx^{1/4} + O(1) \\
& = 2\sqrt{x} \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{n} + A \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} |\chi(n)|\right) \\
& \quad + B \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} 1\right) - 2Bx^{1/4} + O(1) \\
& = 2\sqrt{x} L(1, \chi) + O(1).
\end{aligned}$$

Esto demuestra la parte (b). Es claro que las partes (a) y (b) juntas implican $L(1, \chi) \neq 0$. $\square$

Ejercicios del capítulo 6

1. Sea G el conjunto de las raíces n -ésimas de un número complejo no nulo. Si G es un grupo respecto de la multiplicación, probar que G es el grupo de las raíces n -ésimas de la unidad.
2. Sea G un grupo finito de orden n con elemento identidad e . Si $a_1, \dots, a_n$ son n elementos de G , no necesariamente distintos, probar que existen enteros p y q con $1 \leq p \leq q \leq n$ tales que $a_p a_{p+1} \dots a_q = e$.
3. Sea G el conjunto de todas las matrices $2 \times 2: \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, en donde a, b, c, d son enteros con $ad - bc = 1$. Probar que G es un grupo para la multiplicación de matrices. Este grupo se llama a veces *grupo modular*.
4. Sea $G = \langle a \rangle$ el grupo cíclico engendrado por a . Probar que cada subgrupo de G es cíclico. (No se supone que G es finito.)
5. Sea G un grupo finito de orden n y sea G' un subgrupo de orden m . Probar que $m|n$ (Teorema de Lagrange). Deducir que el orden de cada elemento de G divide a n .
6. Sea G un grupo de orden 6 con elemento identidad e . Probar que o G es cíclico, o existen dos elementos a y b de G tales que

$$G = \{a, a^2, a^3, b, ab, a^2b\},$$

con $a^3 = b^2 = e$. ¿Cuál de estos elementos es ba ?

7. Una tabla de grupo para un grupo finito $G = \{a_1, \dots, a_n\}$ de orden n es una matriz $n \times n$ cuyo elemento ij -ésimo es $a_i a_j$. Si $a_i a_j = e$, probar que $a_j a_i = e$. Con otras palabras, el elemento identidad se halla colocado en la tabla de forma simétrica. Deducir que, si n es par, la ecuación $x^2 = e$ tiene un número par de soluciones.
8. Generalización del ejercicio 7. Si $f(p)$ designa el número de soluciones de la ecuación $x^p = e$, en donde p es un divisor primo de n , el orden de G , probar que $p|f(p)$ (Teorema de Cauchy). [Indicación: Considerar el conjunto S de p -plas ordenadas $(a_1, \dots, a_p)$ tales que $a_i \in G$ y $a_1 \dots a_p = e$. Existen n^{p-1} p -plas en S . Llamamos dos de tales p -plas equivalentes si una es una permutación cíclica de la otra. Probar que $f(p)$ clases de equivalencia contienen exactamente un elemento y que cada una de las otras contiene exactamente p elementos. Contar el número de elementos de S de dos formas y deducir que $p|f(p)$.]

9. Sea G un grupo finito de orden n . Probar que n es impar si, y sólo si, cada elemento de G es un cuadrado. Esto es, si para cada elemento a de G existe un elemento b de G tal que $a = b^2$.
10. Establecer y demostrar una generalización del ejercicio 9 en el que la condición « n es impar» se substituye por « n es primo con k » para un $k \geq 2$.
11. Sea G un grupo finito de orden n , y sea S un subconjunto que contenga más de $n/2$ elementos de G . Probar que para cada g de G existen elementos a y b de S tales que $ab = g$.
12. Sean G un grupo y S un subconjunto de n elementos distintos de G con la propiedad: $a \in S$ implica $a^{-1} \notin S$. Consideremos los n^2 productos (no necesariamente distintos) de la forma ab , en donde $a \in S$ y $b \in S$. Probar que a lo sumo $n(n-1)/2$ de estos productos pertenecen a S .
13. Sean $f_1, \dots, f_m$ los caracteres de un grupo finito G de orden m , y sea a un elemento de G de orden n . El teorema 6.7 establece que cada elemento $f_r(a)$ es una raíz n -ésima de la unidad. Probar que cada raíz n -ésima de la unidad aparece con la misma frecuencia entre los números $f_1(a), \dots, f_m(a)$. [Indicación: Calcular la suma

$$\sum_{r=1}^m \sum_{k=1}^n f_r(a^k) e^{-2\pi i k/n}$$

de dos formas para determinar el número de veces que se presenta $e^{2\pi i/n}$.]

14. Construir tablas que muestren los valores de todos los caracteres de Dirichlet mod k para $k = 8, 9$ y 10 .
15. Sea χ un carácter no principal mod k . Probar que, para todo par de enteros a, b con $a < b$ tenemos

$$\left| \sum_{n=a}^b \chi(n) \right| \leq \frac{1}{2} \varphi(k).$$

16. Sea χ un carácter real mod k , entonces $\chi(n) = \pm 1$ o 0 para cada n , luego la suma

$$S = \sum_{n=1}^k n\chi(n)$$

es un entero. Este ejercicio prueba que $12S \equiv 0 \pmod{k}$.

- (a) Si $(a, k) = 1$ probar que $a\chi(a)S \equiv S \pmod{k}$.
- (b) Escribir $k = 2^a q$ en donde q es impar. Probar que existe un entero a con $(a, k) = 1$ tal que $a \equiv 3 \pmod{2^a}$ y $a \equiv 2 \pmod{q}$. Utilizar entonces (a) para deducir que $12S \equiv 0 \pmod{k}$.
17. Una función aritmética f se llama *periódica* mod k si $k > 0$ y $f(m) = f(n)$ cuando $m \equiv n \pmod{k}$. El entero k se llama el *período* de f .
- (a) Si f es periódica mod k , probar que f admite un período positivo mínimo k_0 y que $k_0 | k$.
- (b) Sea f periódica y completamente multiplicativa, y sea k el menor período positivo de f . Probar que $f(n) = 0$ si $(n, k) > 1$. Esto prueba que f es un carácter de Dirichlet mod k .
18. (a) Sea f un carácter de Dirichlet mod k . Si k carece de cuadrado, probar que k es el menor período positivo de f .
- (b) Dar un ejemplo de un carácter de Dirichlet mod k tal que k no sea el menor período positivo de f .

Capítulo 7

Teorema de Dirichlet relativo a los primos que se encuentran en progresiones aritméticas

7.1 INTRODUCCIÓN

La progresión aritmética de los números impares $1, 3, 5, \dots, 2n+1, \dots$ contiene una infinidad de números primos. Es natural preguntarse si otras progresiones aritméticas poseen esta propiedad. Una progresión aritmética de primer término h y diferencia k consta de todos los números de la forma

$$(1) \quad kn + h, n = 0, 1, 2, \dots$$

Si h y k poseen un divisor d común, cada término de la progresión es divisible por d y, la progresión no podrá contener más de un primo si $d < 1$. Con otras palabras, una condición necesaria para la existencia de infinitos primos en la progresión aritmética (1) es que $(h, k) = 1$. Dirichlet fue el primero que demostró que esta condición también es suficiente. Es decir, si $(h, k) = 1$, la progresión aritmética (1) contiene una infinidad de primos. Este resultado se conoce con el nombre de *teorema de Dirichlet* y lo demostraremos en este capítulo.

Recordemos que Euler demostró la existencia de una infinidad de números primos probando que la serie $\sum p^{-1}$, extendida a todos los primos, diverge. La idea de Dirichlet consiste en demostrar un teorema análogo cuando los primos se hallan obligados a pertenecer a la progresión dada (1). En una famosa memoria [15] publicada en 1837 Dirichlet alcanzó este objetivo por métodos analíticos ingeniosos. Posteriormente la demostración fue simplificada por varios autores. La versión que damos en este capítulo se basa en una demostración de Harold N. Shapiro publicada en 1950 y se refiere, no a la serie $\sum p^{-1}$, sino a la serie $\sum p^{-1} \log p$.

En primer lugar probaremos que, para ciertas progresiones especiales, es fácil demostrar el teorema de Dirichlet modificando la demostración de Euclides relativa a la infinitud de los números primos.

7.2 TEOREMA DE DIRICHLET PARA PRIMOS DE LA FORMA

$$4n - 1 \text{ Y } 4n + 1$$

Teorema 7.1 *Existen infinitos primos de la forma $4n - 1$.*

DEMOSTRACIÓN. Razonamos por contradicción. Suponemos que sólo existe un número finito de tales primos; sea p el mayor de ellos, y consideremos el entero

$$N = 2^2 \cdot 3 \cdot 5 \cdots p - 1.$$

El producto $3 \cdot 5 \cdots p$ contiene todos los primos impares $\leq p$ como factores. Puesto que N es de la forma $4n - 1$ no puede ser primo ya que $N > p$. Ningún primo $\leq p$ divide a N , por lo que todos los factores primos de N exceden a p . Pero no es posible que todos los factores primos de N sean de la forma $4n + 1$ puesto que el producto de dos de tales números es de la misma forma. Luego algún factor primo de N debe ser de la forma $4n - 1$. Esto constituye una contradicción. $\square$

Utilizaremos un tipo diferente de razonamiento para los primos de la forma $4n + 1$.

Teorema 7.2 *Existe una infinitud de primos de la forma $4n + 1$.*

DEMOSTRACIÓN. Sea N un entero > 1 . Probaremos que existe un primo $p > N$ tal que $p \equiv 1 \pmod{4}$. Sea

$$m = (N!)^2 + 1.$$

Obsérvese que m es impar, $m > 1$. Sea p el menor divisor de primo m . Ninguno de los números $2, 3, \dots, N$ divide a m , luego $p > N$. Además tenemos

$$(N!)^2 \equiv -1 \pmod{p}.$$

Elevando ambos miembros a la potencia $(p-1)/2$ obtenemos

$$(N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Pero $(N!)^{p-1} \equiv 1 \pmod{p}$ por el teorema de Euler-Fermat, luego

$$(-1)^{(p-1)/2} \equiv 1 \pmod{p}.$$

Ahora tenemos que la diferencia $(-1)^{(p-1)/2} - 1$ es 0 o -2 , y no puede ser -2 puesto que es divisible por p , por lo que debe ser 0. Esto es,

$$(-1)^{(p-1)/2} = 1.$$

Pero esto significa que $(p-1)/2$ es par, luego $p \equiv 1 \pmod{4}$. Con otras palabras, hemos demostrado que, para cada entero $N > 1$, existe un primo $p > N$ tal que $p \equiv 1 \pmod{4}$. Por consiguiente existe una infinidad de primos de la forma $4n+1$. $\square$

Razonamientos simples como los dados para los primos de la forma $4n-1$ y $4n+1$ se pueden adaptar para tratar otras progresiones aritméticas especiales, tales como $5n-1$, $8n-1$, $8n-3$ y $8n+3$ (ver Sierpinski [67]), sin embargo no se ha encontrado ninguna demostración simple que sirva para la progresión general $kn+h$.

7.3 PLAN DE LA DEMOSTRACIÓN DEL TEOREMA DE DIRICHLET

En el teorema 4.10 obtuvimos la fórmula asintótica

$$(2) \quad \sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$

en donde la suma está extendida a todos los primos $p \leq x$. Probaremos el teorema de Dirichlet como consecuencia de la siguiente fórmula asintótica relacionada con la anterior.

Teorema 7.3 Si $k > 0$ y $(h, k) = 1$, tenemos, para todo $x > 1$,

$$(3) \quad \sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1),$$

en donde la suma se halla extendida a aquellos primos $p \leq x$ que son congruentes con $h \pmod{k}$.

Puesto que $\log x \rightarrow \infty$ cuando $x \rightarrow \infty$, esta relación implica que existe una infinidad de primos $p \equiv h \pmod{k}$, luego una infinidad en la progresión $nk+h$, $n = 0, 1, 2, \dots$

Obsérvese que el término principal de la derecha de (3) es independiente de h . Por consiguiente (3) no sólo implica el teorema de Dirichlet sino que prueba además que los primos en cada una de las $\varphi(k)$ clases de restos reducidos mod k , tienen la misma participación en el término principal de (2).

La demostración del teorema 7.3 se presentará a través de una sucesión de lemas que hemos colocado juntos en esta sección para poner de relieve el plan de la demostración. A lo largo del capítulo adoptaremos la siguiente notación.

El entero positivo k representa un módulo fijo, y h un entero fijo primo con k . Los $\varphi(k)$ caracteres de Dirichlet mod k se designarán por

$$\chi_1, \chi_2, \dots, \chi_{\varphi(k)}$$

en donde χ_1 designa el carácter principal. Para $\chi \neq \chi_1$ escribimos $L(1, \chi)$ y $L'(1, \chi)$ para designar las sumas de las siguientes series:

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n},$$

$$L'(1, \chi) = - \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n}.$$

La convergencia de cada una de estas series se estableció en el teorema 6.18. Además, en el teorema 6.20 se estableció que $L(1, \chi) \neq 0$ si χ es una función real. El símbolo p designa un primo, y $\sum_{p \leq x}$ designa la suma extendida a todos los primos $p \leq x$.

Lema 7.4 Para cada $x > 1$ tenemos

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + O(1).$$

Es claro que el lema 7.4 implica el teorema 7.3 si probamos que

$$(4) \quad \sum_{p \leq x} \frac{\chi(p) \log p}{p} = O(1)$$

para cada $\chi \neq \chi_1$. El lema que sigue expresa esta suma en una forma que no está extendida a los primos.

Lema 7.5 Para $x > 1$ y $\chi \neq \chi_1$ tenemos

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} = -L'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(1).$$

Por consiguiente el lema 7.5 implicará (4) si demostramos que

$$(5) \quad \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} = O(1).$$

Esto, a su vez, se deducirá del siguiente lema.

Lema 7.6 Para $x > 1$ y $\chi \neq \chi_1$ tenemos

$$(6) \quad L(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} = O(1).$$

Si $L(1, \chi) \neq 0$ podemos eliminar $L(1, \chi)$ en (6) a fin de obtener (5). Por consiguiente, la demostración del teorema de Dirichlet depende en última instancia de la no anulación de $L(1, \chi)$ para todo $\chi \neq \chi_1$. Como ya hemos hecho notar, en el teorema 6.20 se demostró este resultado para χ real $\neq \chi_1$, por lo que únicamente debemos demostrar que $L(1, \chi) \neq 0$ para $\chi \neq \chi_1$ tanto si toma valores reales como complejos.

A este fin sea $N(k)$ el número de caracteres no principales $\chi \bmod k$ tales que $L(1, \chi) = 0$. Si $L(1, \chi) = 0$ entonces $L(1, \bar{\chi}) = 0$ y $\chi \neq \bar{\chi}$ puesto que χ no es real. Por consiguiente los caracteres χ para los que $L(1, \chi) = 0$ intervienen por pares conjugados, luego $N(k)$ es par. Nuestro propósito consiste en demostrar que $N(k) = 0$, y esto se deduce de la fórmula asintótica que sigue.

Lema 7.7 Para $x > 1$ tenemos

$$(7) \quad \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{k}}} \frac{\log p}{p} = \frac{1 - N(k)}{\varphi(k)} \log x + O(1).$$

Si $N(k) \neq 0$ entonces $N(k) \geq 2$ ya que $N(k)$ es par, luego el coeficiente de $\log x$ en (7) es negativo y en el segundo el miembro tiende a $-\infty$ cuando $x \rightarrow \infty$. Esto es una contradicción ya que todos los términos del primer miembro son positivos.

Por consiguiente el lema 7.7 implica $N(k) = 0$. La demostración del lema 7.7 a su vez, se basa en la siguiente fórmula asintótica.

Lema 7.8 Si $\chi \neq \chi_1$ y $L(1, \chi) = 0$ tenemos

$$L'(1, \chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} = \log x + O(1).$$

7.4 DEMOSTRACIÓN DEL LEMA 7.4

Para probar el lema 7.4 empezamos por la fórmula asintótica mencionada anteriormente,

$$(2) \quad \sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$$

y extraemos aquellos términos de la suma que provienen de los primos $p \equiv h \pmod{k}$. La extracción se efectúa con la ayuda de la relación de ortogonalidad para caracteres de Dirichlet, tal como expresa el teorema 6.16:

$$\sum_{r=1}^{\varphi(k)} \chi_r(m) \bar{\chi}_r(n) = \begin{cases} \varphi(k) & \text{si } m \equiv n \pmod{k}, \\ 0 & \text{si } m \not\equiv n \pmod{k}. \end{cases}$$

Esto es válido para $(n, k) = 1$. Tomamos $m = p$ y $n = h$, en donde $(h, k) = 1$, y multiplicamos los dos miembros por $p^{-1} \log p$ y sumamos para todo $p \leq x$ para obtener

$$(8) \quad \sum_{p \leq x} \sum_{r=1}^{\varphi(k)} \chi_r(p) \bar{\chi}_r(h) \frac{\log p}{p} = \varphi(k) \sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p}.$$

En la suma de la izquierda aislamos aquellos términos que contienen únicamente el carácter principal χ_1 y escribimos (8) en la forma

$$(9) \quad \varphi(k) \sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \bar{\chi}_1(h) \sum_{p \leq x} \frac{\chi_1(p) \log p}{p} + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p}.$$

Ahora bien $\bar{\chi}_1(h) = 1$ y $\chi_1(p) = 0$ a menos que $(p, k) = 1$, en cuyo caso $\chi_1(p) = 1$. Por lo tanto el primer término del segundo miembro de (9) viene dado por

$$(10) \quad \sum_{\substack{p \leq x \\ (p, k) = 1}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} - \sum_{\substack{p \leq x \\ p|k}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} + O(1),$$

puesto que sólo existe un número finito de primos que divida a k . Combinando (10) con (9) obtenemos

$$\varphi(k) \sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + O(1).$$

Utilizando (2) y dividiendo por $\varphi(k)$ obtenemos el lema 7.4. □

7.5 DEMOSTRACIÓN DEL LEMA 7.5

Empezaremos con la suma

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n},$$

en donde $\Lambda(n)$ es la función de Mangoldt, y expresaremos esta suma de dos formas diferentes. En primer lugar observamos que la definición de $\Lambda(n)$ nos proporciona

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = \sum_{\substack{p \leq x \\ p^a \leq x}} \sum_{a=1}^{\infty} \frac{\chi(p^a) \log p}{p^a}.$$

Separamos los términos con $a = 1$ y escribimos

$$(11) \quad \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = \sum_{p \leq x} \frac{\chi(p) \log p}{p} + \sum_{\substack{p \leq x \\ p^a \leq x \\ a \geq 2}} \sum_{a=2}^{\infty} \frac{\chi(p^a) \log p}{p^a}.$$

La segunda suma de la derecha está acotada superiormente por

$$\sum_p \log p \sum_{a=2}^{\infty} \frac{1}{p^a} = \sum_p \frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1),$$

con lo que (11) nos da

$$(12) \quad \sum_{p \leq x} \frac{\chi(p) \log p}{p} = \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} + O(1).$$

Ahora recordamos que $\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d)$, luego

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log \frac{n}{d}.$$

En la última suma escribimos $n = cd$ y utilizamos la propiedad multiplicativa de χ para obtener

$$(13) \quad \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} \sum_{c \leq x/d} \frac{\chi(c) \log c}{c}.$$

Dado que $x/d \geq 1$, en la suma respecto de c podemos utilizar la fórmula (10) del teorema 6.18 para obtener

$$\sum_{c \leq x/d} \frac{\chi(c) \log c}{c} = -L'(1, \chi) + O\left(\frac{\log x/d}{x/d}\right).$$

La ecuación (13) se convierte ahora en

$$(14) \quad \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = -L'(1, \chi) \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} + O\left(\sum_{d \leq x} \frac{1}{d} \frac{\log x/d}{x/d}\right).$$

La suma del O -término es

$$\frac{1}{x} \sum_{d \leq x} (\log x - \log d) = \frac{1}{x} \left([x] \log x - \sum_{d \leq x} \log d \right) = O(1)$$

puesto que

$$\sum_{d \leq x} \log d = \log[x]! = x \log x + O(x).$$

Por lo tanto (14) se transforma en

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = -L'(1, \chi) \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} + O(1)$$

que, con (12), prueba el lema 7.5.

7.6 DEMOSTRACIÓN DEL LEMA 7.6

Utilizamos la fórmula de inversión de Möbius generalizada demostrada en el teorema 2.23 que establece que, si α es completamente multiplicativo, tenemos

$$(15) \quad G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \quad \text{si, y sólo si} \quad F(x) = \sum_{n \leq x} \mu(n) \alpha(n) G\left(\frac{x}{n}\right).$$

Hacemos $\alpha(n) = \chi(n)$ y $F(x) = x$ para obtener

$$(16) \quad x = \sum_{n \leq x} \mu(n) \chi(n) G\left(\frac{x}{n}\right)$$

en donde

$$G(x) = \sum_{n \leq x} \chi(n) \frac{x}{n} = x \sum_{n \leq x} \frac{\chi(n)}{n}.$$

Por la ecuación (9) del teorema 6.18 podemos escribir $G(x) = xL(1, \chi) + O(1)$. Utilizamos este resultado en (16) y hallamos

$$x = \sum_{n \leq x} \mu(n) \chi(n) \left\{ \frac{x}{n} L(1, \chi) + O(1) \right\} = xL(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(x).$$

Ahora dividimos por x para obtener el lema 7.6. □

7.7 DEMOSTRACIÓN DEL LEMA 7.8

Probaremos el lema 7.8 y lo utilizaremos para demostrar el lema 7.7. De nuevo haremos uso de la fórmula de inversión de Möbius generalizada (15). Esta vez tomamos $F(x) = x \log x$ para obtener

$$(17) \quad x \log x = \sum_{n \leq x} \mu(n) \chi(n) G\left(\frac{x}{n}\right)$$

en donde

$$G(x) = \sum_{n \leq x} \chi(n) \frac{x}{n} \log \frac{x}{n} = x \log x \sum_{n \leq x} \frac{\chi(n)}{n} - x \sum_{n \leq x} \frac{\chi(n) \log n}{n}.$$

Ahora utilizamos las fórmulas (9) y (10) del teorema 6.18 para conseguir

$$\begin{aligned} G(x) &= x \log x \left\{ L(1, \chi) + O\left(\frac{1}{x}\right) \right\} + x \left\{ L'(1, \chi) + O\left(\frac{\log x}{x}\right) \right\} \\ &= xL'(1, \chi) + O(\log x) \end{aligned}$$

ya que hemos supuesto que $L(1, \chi) = 0$. Por lo que (17) nos da

$$\begin{aligned} x \log x &= \sum_{n \leq x} \mu(n) \chi(n) \left\{ \frac{x}{n} L'(1, \chi) + O\left(\log \frac{x}{n}\right) \right\} \\ &= xL'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O\left(\sum_{n \leq x} (\log x - \log n)\right). \end{aligned}$$

Hemos observado ya que el O -término de la derecha es $O(x)$ (ver la demostración del lema 7.5). Por lo tanto tenemos

$$x \log x = xL'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(x),$$

y cuando dividimos por x obtenemos el lema 7.8. □

7.8 DEMOSTRACIÓN DEL LEMA 7.7

Utilizamos el lema 7.4 con $h = 1$ para conseguir

$$(18) \quad \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + O(1).$$

En la suma relativa a p de la derecha utilizamos el lema 7.5 que establece

$$\sum_{p \leq x} \frac{\chi_r(p) \log p}{p} = -L'(1, \chi_r) \sum_{n \leq x} \frac{\mu(n) \chi_r(n)}{n} + O(1).$$

Si $L(1, \chi_r) \neq 0$ el lema 7.6 prueba que el miembro de la derecha de (18) es $O(1)$. Pero si $L(1, \chi_r) = 0$ entonces el lema 7.8 implica

$$-L'(1, \chi_r) \sum_{n \leq x} \frac{\mu(n) \chi_r(n)}{n} = -\log x + O(1).$$

Por consiguiente la suma de la derecha de (18) es

$$\frac{1}{\varphi(k)} \{-N(k) \log x + O(1)\},$$

luego (18) se transforma en

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{k}}} \frac{\log p}{p} = \frac{1 - N(k)}{\varphi(k)} \log x + O(1).$$

Esto demuestra el lema 7.7 y por consiguiente demuestra también el teorema 7.3. $\square$

Como hemos observado anteriormente, el teorema 7.3 implica el teorema de Dirichlet:

Teorema 7.9 Si $k > 0$ y $(h, k) = 1$, existe una infinidad de primos en la progresión aritmética $nk + h$, $n = 0, 1, 2, \dots$

7.9 DISTRIBUCIÓN DE PRIMOS EN PROGRESIONES ARITMÉTICAS

Si $k > 0$ y $(a, k) = 1$, sea

$$\pi_a(x) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{k}}} 1.$$

La función $\pi_a(x)$ cuenta el número de primos $\leq x$ en la progresión $nk + a$, $n = 0, 1, 2, \dots$. El teorema de Dirichlet prueba que $\pi_a(x) \rightarrow \infty$ cuando $x \rightarrow \infty$. Existe además un teorema del número primo para progresiones aritméticas que establece que

$$(19) \quad \pi_a(x) \sim \frac{\pi(x)}{\varphi(k)} \sim \frac{1}{\varphi(k)} \frac{x}{\log x} \quad \text{cuando } x \rightarrow \infty,$$

si $(a, k) = 1$. En [44] se exponen las líneas generales de una demostración de (19). La fórmula del teorema 7.3,

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1).$$

sugiere el teorema del número primo para progresiones. Dado que la parte principal es independiente de h , los primos aparecen igualmente repartidos entre las $\varphi(k)$ clases residuales reducidas mod k , y (19) establece con precisión este hecho.

Concluiremos este capítulo dando otra formulación del teorema del número primo para progresiones aritméticas.

Teorema 7.10 *Si la relación*

$$(20) \quad \pi_a(x) \sim \frac{\pi(x)}{\varphi(k)} \quad \text{cuando } x \rightarrow \infty$$

se verifica para todo entero primo con k , entonces

$$(21) \quad \pi_a(x) \sim \pi_b(x) \quad \text{cuando } x \rightarrow \infty$$

siempre que $(a, k) = (b, k) = 1$. Recíprocamente, (21) implica (20).

DEMOSTRACIÓN. Es claro que (20) implica (21). Para demostrar el recíproco suponemos que se verifica (21) y que $A(k)$ designa el número de primos que dividen a k . Si $x > k$ tenemos

$$\begin{aligned} \pi(x) &= \sum_{p \leq x} 1 = A(k) + \sum_{\substack{p \leq x \\ p \nmid k}} 1 \\ &= A(k) + \sum_{\substack{a=1 \\ (a, k)=1}}^k \sum_{\substack{p \leq x \\ p \equiv a \pmod{k}}} 1 = A(k) + \sum_{\substack{a=1 \\ (a, k)=1}}^k \pi_a(x). \end{aligned}$$

Por consiguiente

$$\frac{\pi(x) - A(k)}{\pi_b(x)} = \sum_{\substack{a=1 \\ (a, k)=1}}^k \frac{\pi_a(x)}{\pi_b(x)}.$$

Por (21) cada término de la suma tiende a 1 cuando $x \rightarrow \infty$, luego la suma tiende a $\varphi(k)$. Luego

$$\frac{\pi(x)}{\pi_b(x)} - \frac{A(k)}{\pi_b(x)} \rightarrow \varphi(k) \quad \text{cuando } x \rightarrow \infty.$$

Pero $A(k)/\pi_b(x) \rightarrow 0$ luego $\pi(x)/\pi_b(x) \rightarrow \varphi(k)$, que prueba (20). $\square$

Ejercicios del capítulo 7

En los ejercicios del 1 al 4, h y k son enteros positivos dados, $(h, k) = 1$, y $A(h, k)$ es la progresión aritmética $A(h, k) = \{h + kx : x = 0, 1, 2, \dots\}$. Los ejercicios del 1 al 4 deben resolverse sin utilizar el teorema de Dirichlet.

1. Probar que, para cada entero $n \geq 1$, $A(h, k)$ contiene una infinidad de números primos con n .
2. Probar que $A(h, k)$ contiene un subconjunto infinito $\{a_1, a_2, \dots\}$ tal que $(a_i, a_j) = 1$ si $i \neq j$.
3. Probar que $A(h, k)$ contiene un subconjunto infinito que forma una progresión geométrica (un conjunto de números de la forma ar^n , $n = 0, 1, 2, \dots$). Ello implica que $A(h, k)$ contiene una infinidad de números que tienen los mismos factores primos.
4. Sea S un subconjunto infinito de $A(h, k)$. Probar que para cada entero positivo n existe un número en $A(h, k)$ que se puede expresar como producto de más de n elementos distintos de S .
5. El teorema de Dirichlet implica la siguiente afirmación: Si h y $k > 0$ son dos enteros tales que $(h, k) = 1$, entonces por lo menos existe un primo de la forma $kn + h$. Probar que esta afirmación implica también el teorema de Dirichlet.
6. Si $(h, k) = 1$, $k > 0$, probar que existe una constante A (que depende de h y de k) tal que, si $x \geq 2$,

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{1}{p} = \frac{1}{\varphi(k)} \log \log x + A + O\left(\frac{1}{\log x}\right).$$

7. Construir un conjunto infinito S de números primos que verifique la siguiente propiedad: Si $p \in S$ y $q \in S$ entonces $(\frac{1}{2}(p-1), \frac{1}{2}(q-1)) = (p, q-1) = (p-1, q) = 1$.
8. Sea f un polinomio de grado $n \geq 1$ con coeficientes enteros que verifique la siguiente propiedad: Para cada primo p existe un primo q y un entero m tales que $f(p) = q^m$. Probar que $q = p$, $m = n$ y $f(x) = x^n$ para todo x . [Indicación: Si $q \neq p$, entonces q^{m+1} divide a $f(p + tq^{m+1}) - f(p)$ para cada $t = 1, 2, \dots$]

Capítulo 8

Funciones aritméticas periódicas y sumas de Gauss

8.1 FUNCIONES PERIÓDICAS MÓDULO k

Sea k un entero positivo. Una función aritmética f se llama *periódica de período k* (o *periódica módulo k*) si

$$f(n+k) = f(n)$$

para todo entero n . Si k es un período lo es mk para todo entero $m > 0$. El menor período positivo de f se llama el *período fundamental*.

Las funciones periódicas han aparecido ya en capítulos anteriores. Por ejemplo, los caracteres de Dirichlet mod k son periódicos mod k . Un ejemplo simple es el máximo común divisor (n, k) considerado como función de n . La periodicidad se introduce a través de la relación

$$(n+k, k) = (n, k).$$

Otro ejemplo es la función exponencial

$$f(n) = e^{2\pi i m n / k}$$

en donde m y k son enteros fijos. El número $e^{2\pi i m / k}$ es una raíz k -ésima de la unidad y $f(n)$ es su n -ésima potencia. Toda combinación lineal finita de tales funciones,

$$\sum_m c(m) e^{2\pi i m n / k}$$

también es periódica mod k para cada elección de los coeficientes $c(m)$. Nuestro primer propósito consiste en demostrar que cada función aritmética periódica mod k se puede expresar como una combinación lineal de este tipo. Estas sumas se llaman *series finitas de Fourier*. Empezaremos este análisis con un ejemplo simple pero importante conocido con el nombre de *suma geométrica*.

Teorema 8.1 Para $k \geq 1$ fijado, sea

$$g(n) = \sum_{m=0}^{k-1} e^{2\pi i mn/k}.$$

Entonces

$$g(n) = \begin{cases} 0 & \text{si } k \nmid n, \\ k & \text{si } k|n. \end{cases}$$

DEMOSTRACIÓN. Dado que $g(n)$ es la suma de los términos de una progresión geométrica,

$$g(n) = \sum_{m=0}^{k-1} x^m,$$

en donde $x = e^{2\pi i n/k}$ tenemos

$$g(n) = \begin{cases} \frac{x^k - 1}{x - 1} & \text{si } x \neq 1, \\ k & \text{si } x = 1. \end{cases}$$

Pero $x^k = 1$, y $x = 1$ si, y sólo si, $k|n$, luego el teorema queda demostrado. $\square$

8.2 EXISTENCIA DE SERIES FINITAS DE FOURIER PARA FUNCIONES ARITMÉTICAS PERIÓDICAS

Utilizaremos la fórmula de interpolación polinómica de Lagrange para demostrar que cada función aritmética periódica posee un desarrollo finito de Fourier.

Teorema 8.2 Teorema de interpolación de Lagrange. Sean $z_0, z_1, \dots, z_{k-1}$, k números complejos distintos, y sean $w_0, w_1, \dots, w_{k-1}$, k números complejos no nece-

sariamente distintos. Entonces existe un único polinomio $P(z)$ de grado $\leq k-1$ tal que

$$P(z_m) = w_m \quad \text{para } m = 0, 1, 2, \dots, k-1.$$

DEMOSTRACIÓN. El polinomio requerido $P(z)$, llamado polinomio de interpolación de Lagrange, se puede construir explícitamente como sigue. Sea

$$A(z) = (z - z_0)(z - z_1) \cdots (z - z_{k-1})$$

y sea

$$A_m(z) = \frac{A(z)}{z - z_m}.$$

Entonces $A_m(z)$ es un polinomio de grado $k-1$ con las propiedades siguientes:

$$A_m(z_m) \neq 0, \quad A_m(z_j) = 0 \quad \text{si } j \neq m.$$

Por lo tanto $A_m(z)/A_m(z_m)$ es un polinomio de grado $k-1$ que se anula en cada z_j para $j \neq m$, y que toma el valor 1 en z_m . Por consiguiente la combinación lineal

$$P(z) = \sum_{m=0}^{k-1} w_m \frac{A_m(z)}{A_m(z_m)}$$

es un polinomio de grado $\leq k-1$ con $P(z_j) = w_j$ para cada j . Si existiese otro polinomio $Q(z)$ como éste, la diferencia $P(z) - Q(z)$ se anularía en k puntos distintos, luego $P(z) = Q(z)$ ya que ambos polinomios tienen grado $\leq k-1$. $\square$

Ahora elegimos como números $z_0, z_1, \dots, z_{k-1}$ las raíces k -ésimas de la unidad y obtenemos:

Teorema 8.3 *Dados k números complejos $w_0, w_1, \dots, w_{k-1}$, existen k números complejos unívocamente determinados $a_0, a_1, \dots, a_{k-1}$ tales que*

$$(1) \quad w_m = \sum_{n=0}^{k-1} a_n e^{2\pi i m n / k}$$

para $m = 0, 1, 2, \dots, k-1$. Además, los coeficientes a_n vienen expresados por la fórmula

$$(2) \quad a_n = \frac{1}{k} \sum_{m=0}^{k-1} w_m e^{-2\pi i m n/k} \quad \text{para } n = 0, 1, 2, \dots, k-1.$$

DEMOSTRACIÓN. Sea $z_m = e^{2\pi i m/k}$. Los números $z_0, z_1, \dots, z_{k-1}$ son distintos, luego existe un único polinomio de Lagrange

$$P(z) = \sum_{n=0}^{k-1} a_n z^n$$

tal que $P(z_m) = w_m$ para cada $m = 0, 1, \dots, k-1$. Ello demuestra que existen números a_n , unívocamente determinados, que verifican (1). Para deducir la fórmula (2) para a_n multiplicamos ambos miembros de (1) por $e^{-2\pi i m r/k}$, en donde m y r son enteros no negativos menores que k , y sumando respecto a m obtenemos

$$\sum_{m=0}^{k-1} w_m e^{-2\pi i m r/k} = \sum_{n=0}^{k-1} a_n \sum_{m=0}^{k-1} e^{2\pi i (n-r)m/k}.$$

Por el teorema 8.1, la suma respecto a m es 0 a menos que $k|(n-r)$. Pero $|n-r| \leq k-1$ luego $k|(n-r)$ si, y sólo si, $n=r$. Por consiguiente los únicos términos que no se anulan en el miembro de la derecha aparecen cuando $n=r$ y obtenemos

$$\sum_{m=0}^{k-1} w_m e^{-2\pi i m r/k} = k a_r.$$

Esta ecuación nos da (2). □

Teorema 8.4 *Sea f una función aritmética periódica mod k . Entonces existe una función aritmética g unívocamente determinada, también periódica mod k , tal que*

$$f(m) = \sum_{n=0}^{k-1} g(n) e^{2\pi i m n/k}.$$

De hecho g viene expresada por la fórmula

$$g(n) = \frac{1}{k} \sum_{m=0}^{k-1} f(m) e^{-2\pi i m n/k}.$$

DEMOSTRACIÓN. Sea $w_m = f(m)$ para $m = 0, 1, 2, \dots, k-1$ y apliquemos el teorema 3.8 para determinar los números $a_0, a_1, \dots, a_{k-1}$. Definimos la función g por medio de las relaciones $g(m) = a_m$ para $m = 0, 1, 2, \dots, k-1$ y extendemos la definición de $g(m)$ a todos los enteros m por periodicidad mod k . Entonces f se halla relacionada con g por las ecuaciones del teorema. $\square$

Nota. Puesto que tanto f como g son periódicas mod k podemos escribir las sumas del teorema 8.4 como sigue:

$$(3) \quad f(m) = \sum_{n \bmod k} g(n) e^{2\pi i m n / k}$$

y

$$(4) \quad g(n) = \frac{1}{k} \sum_{m \bmod k} f(m) e^{-2\pi i m n / k}.$$

En cada caso la suma se puede extender a un sistema residual completo mod k . La suma de (3) se llama *desarrollo finito de Fourier* de f y los números $g(n)$ definidos por (4) se llaman *coeficientes de Fourier* de f .

8.3 SUMA DE RAMANUJAN Y GENERALIZACIONES

En el ejercicio 2.14(b) hemos demostrado que la función de Möbius $\mu(k)$ es la suma de la k -ésimas raíces primitivas de la unidad. En esta sección generalizaremos este resultado. Concretando, sea n un entero positivo prefijado y consideremos la suma de las potencias n -ésimas de las raíces primitivas k -ésimas de la unidad. Esta suma se conoce como *suma de Ramanujan* y se designa $c_k(n)$:

$$c_k(n) = \sum_{\substack{m \bmod k \\ (m, k) = 1}} e^{2\pi i m n / k}.$$

Ya hemos indicado que, cuando $n = 1$, esta suma se reduce a la función de Möbius,

$$\mu(k) = c_k(1).$$

Cuando $k|n$ la suma se reduce a la función φ de Euler ya que cada término es 1 y el número de términos es $\varphi(k)$. Ramanujan demostró que $c_k(n)$ es siempre un

entero y que posee propiedades multiplicativas interesantes. Dedujo estos hechos de la relación

$$(5) \quad c_k(n) = \sum_{d|(n, k)} d\mu\left(\frac{k}{d}\right).$$

Esta fórmula muestra como de $c_k(n)$ se llega a $\mu(k)$ y a $\varphi(k)$. En efecto, cuando $n = 1$ sólo existe un término en la suma y obtenemos $c_k(1) = \mu(k)$. Y cuando $k|n$ tenemos $(n, k) = k$ y $c_k(n) = \sum_{d|n} d\mu(k/d) = \varphi(k)$. Deduciremos (5) como un caso especial de un resultado más general (teorema 8.5).

La fórmula (5) para $c_k(n)$ sugiere estudiar sumas generales de la forma

$$(6) \quad \sum_{d|(n, k)} f(d)g\left(\frac{k}{d}\right).$$

Éstas se parecen a las sumas de la convolución de Dirichlet $f * g$ excepto que la suma se halla extendida a un *subconjunto* de los divisores de k , a saber a los d que también dividen a n .

La suma de (6) la designamos por $s_k(n)$. Puesto que n sólo interviene en el mcd (n, k) tenemos

$$s_k(n + k) = s_k(n)$$

por lo tanto $s_k(n)$ es una función periódica de n , de período k . Luego esta suma admite un desarrollo finito de Fourier. El teorema que sigue nos dice que sus coeficientes de Fourier vienen dados por una suma del mismo tipo.

Teorema 8.5 Sea $s_k(n) = \sum_{d|(n, k)} f(d)g(k/d)$. Entonces $s_k(n)$ admite el desarrollo finito de Fourier

$$(7) \quad s_k(n) = \sum_{m \bmod k} a_k(m) e^{2\pi i m n / k}$$

en donde

$$(8) \quad a_k(m) = \sum_{d|(m, k)} g(d)f\left(\frac{k}{d}\right)\frac{d}{k}.$$

DEMOSTRACIÓN. Por el teorema 8.4, los coeficientes $a_k(m)$ se obtienen por

$$\begin{aligned}
 a_k(m) &= \frac{1}{k} \sum_{n \bmod k} s_k(n) e^{-2\pi i n m / k} \\
 &= \frac{1}{k} \sum_{n=1}^k \sum_{\substack{d|n \\ d|k}} f(d) g\left(\frac{k}{d}\right) e^{-2\pi i n m / k}.
 \end{aligned}$$

Ahora escribimos $n = cd$ y observamos que, para cada d , el índice c recorre los valores de 1 a k/d y obtenemos

$$a_k(m) = \frac{1}{k} \sum_{d|k} f(d) g\left(\frac{k}{d}\right) \sum_{c=1}^{k/d} e^{-2\pi i c d m / k}.$$

Ahora sustituimos k/d por d en la suma de la derecha para obtener

$$a_k(m) = \frac{1}{k} \sum_{\substack{d|k \\ d|m}} f\left(\frac{k}{d}\right) g(d) \sum_{c=1}^d e^{-2\pi i c m / d}.$$

Pero, en virtud del teorema 8.1 la suma relativa a c es 0 salvo para $d|m$ en cuyo caso la suma vale d . Luego

$$a_k(m) = \frac{1}{k} \sum_{\substack{d|k \\ d|m}} f\left(\frac{k}{d}\right) g(d) d$$

que prueba (8). □

Ahora, particularizando f y g , obtenemos la fórmula de la suma de Ramanujan mencionada anteriormente.

Teorema 8.6 *Tenemos*

$$c_k(n) = \sum_{d|(n, k)} d \mu\left(\frac{k}{d}\right).$$

DEMOSTRACIÓN. Haciendo $f(k) = k$ y $g(k) = \mu(k)$ en el teorema 8.5 resulta

$$\sum_{d|(n, k)} d \mu\left(\frac{k}{d}\right) = \sum_{m \bmod k} a_k(m) e^{2\pi i m n / k}$$

en donde

$$a_k(m) = \sum_{d|(m,k)} \mu(d) = \left[\frac{1}{(m,k)} \right] = \begin{cases} 1 & \text{si } (m,k) = 1, \\ 0 & \text{si } (m,k) > 1. \end{cases}$$

Luego

$$\sum_{d|(n,k)} d \mu\left(\frac{k}{d}\right) = \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi i mn/k} = c_k(n). \quad \square$$

8.4 PROPIEDADES MULTIPLICATIVAS DE LAS SUMAS $s_k(n)$

Teorema 8.7 Sea

$$s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right)$$

en donde f y g son multiplicativas. Entonces tenemos

$$(9) \quad s_{mk}(ab) = s_m(a)s_k(b) \quad \text{siempre que } (a,k) = (b,m) = 1.$$

En particular es

$$(10) \quad s_m(ab) = s_m(a) \quad \text{si } (b,m) = 1,$$

y

$$(11) \quad s_{mk}(a) = s_m(a)g(k) \quad \text{si } (a,k) = 1.$$

DEMOSTRACIÓN. Las relaciones $(a,k) = (b,m) = 1$ implican (ver ejercicio 1.24)

$$(mk, ab) = (a, m)(k, b)$$

siendo (a, m) y (b, k) primos entre sí. Por consiguiente

$$s_{mk}(ab) = \sum_{d|(mk, ab)} f(d)g\left(\frac{mk}{d}\right) = \sum_{d|(a, m)(b, k)} f(d)g\left(\frac{mk}{d}\right).$$

Si, en la última suma, escribimos $d = d_1 d_2$ se obtiene

$$\begin{aligned}
 s_{mk}(ab) &= \sum_{d_1|(a,m)} \sum_{d_2|(b,k)} f(d_1 d_2) g\left(\frac{mk}{d_1 d_2}\right) \\
 &= \sum_{d_1|(a,m)} f(d_1) g\left(\frac{m}{d_1}\right) \sum_{d_2|(b,k)} f(d_2) g\left(\frac{k}{d_2}\right) = s_m(a) s_k(b).
 \end{aligned}$$

Ello prueba (9).

Si, en (9), hacemos $k = 1$ se obtiene

$$s_m(ab) = s_m(a) s_1(b) = s_m(a)$$

ya que $s_1(b) = f(1)g(1) = 1$. Esto prueba (10). Si hacemos $b = 1$ en (9) obtenemos

$$s_{mk}(a) = s_m(a) s_k(1) = s_m(a) g(k)$$

ya que $s_k(1) = f(1)g(k) = g(k)$. Esto demuestra (11). $\square$

EJEMPLO Aplicando la suma de Ramanujan obtenemos las siguientes propiedades multiplicativas:

$$\begin{aligned}
 c_{mk}(ab) &= c_m(a) c_k(b) & \text{si } (a, k) &= (b, m) = 1, \\
 c_m(ab) &= c_m(a) & \text{si } (b, m) &= 1,
 \end{aligned}$$

y

$$c_{mk}(a) = c_m(a) \mu(k) \quad \text{si } (a, k) = 1.$$

A veces las sumas $s_k(n)$ se pueden evaluar en términos de la convolución de Dirichlet $f * g$. A este respecto tenemos:

Teorema 8.8 Sea f completamente multiplicativa, y sea $g(k) = \mu(k)h(k)$, en donde h es multiplicativa. Supongamos que $f(p) \neq 0$ y que $f(p) \neq h(p)$ para todo primo p , y sea

$$s_k(n) = \sum_{d|(n,k)} f(d) g\left(\frac{k}{d}\right).$$

Entonces tenemos

$$s_k(n) = \frac{F(k)g(N)}{F(N)},$$

en donde $F = f * g$ y $N = k/(n, k)$.

DEMOSTRACIÓN. Observemos en primer lugar

$$\begin{aligned} F(k) &= \sum_{d|k} f(d) \mu\left(\frac{k}{d}\right) h\left(\frac{k}{d}\right) = \sum_{d|k} f\left(\frac{k}{d}\right) \mu(d) h(d) = f(k) \sum_{d|k} \mu(d) \frac{h(d)}{f(d)} \\ &= f(k) \prod_{p|k} \left(1 - \frac{h(p)}{f(p)}\right). \end{aligned}$$

A continuación hagamos $a = (n, k)$, o sea que $k = aN$. Entonces tenemos

$$\begin{aligned} s_k(n) &= \sum_{d|a} f(d) \mu\left(\frac{k}{d}\right) h\left(\frac{k}{d}\right) = \sum_{d|a} f(d) \mu\left(\frac{aN}{d}\right) h\left(\frac{aN}{d}\right) \\ &= \sum_{d|a} f\left(\frac{a}{d}\right) \mu(Nd) h(Nd). \end{aligned}$$

Pero $\mu(Nd) = \mu(N)\mu(d)$ si $(N, d) = 1$, y $\mu(Nd) = 0$ si $(N, d) > 1$, luego la última ecuación nos da

$$\begin{aligned} s_k(n) &= \mu(N)h(N) \sum_{\substack{d|a \\ (N, d)=1}} f\left(\frac{a}{d}\right) \mu(d) h(d) = f(a)\mu(N)h(N) \sum_{\substack{d|a \\ (N, d)=1}} \mu(d) \frac{h(d)}{f(d)} \\ &= f(a)\mu(N)h(N) \prod_{\substack{p|a \\ p \nmid N}} \left(1 - \frac{h(p)}{f(p)}\right) = f(a)\mu(N)h(N) \frac{\prod_{p|aN} \left(1 - \frac{h(p)}{f(p)}\right)}{\prod_{p|N} \left(1 - \frac{h(p)}{f(p)}\right)} \\ &= f(a)\mu(N)h(N) \frac{F(k)}{f(k)} \frac{f(N)}{F(N)} = \frac{F(k)\mu(N)h(N)}{F(N)} = \frac{F(k)g(N)}{F(N)}. \quad \square \end{aligned}$$

EJEMPLO Para sumas de Ramanujan obtenemos la siguiente simplificación:

$$c_k(n) = \varphi(k)\mu(N)/\varphi(N) = \frac{\varphi(k)\mu\left(\frac{k}{(n, k)}\right)}{\varphi\left(\frac{k}{(n, k)}\right)}.$$

8.5 SUMAS DE GAUSS ASOCIADAS A CARACTERES DE DIRICHLET

Definición. Para todo carácter de Dirichlet $\chi \bmod k$, la suma

$$G(n, \chi) = \sum_{m=1}^k \chi(m) e^{2\pi i mn/k}$$

se llama suma de Gauss asociada a χ .

Si $\chi = \chi_1$ es el carácter principal mod k , tenemos $\chi_1(m) = 1$ si $(m, k) = 1$, y $\chi_1(m) = 0$ en otro caso. Para este carácter la suma de Gauss se reduce a la suma de Ramanujan:

$$G(n, \chi_1) = \sum_{\substack{m=1 \\ (m, k)=1}}^k e^{2\pi i mn/k} = c_k(n).$$

Luego la suma de Gauss $G(n, \chi)$ se puede considerar una generalización de la suma de Ramanujan. Ahora efectuamos un estudio detallado de sus propiedades.

El primer resultado es una propiedad de factorización que juega un papel importante en todo el desarrollo subsiguiente.

Teorema 8.9 Si χ es un carácter de Dirichlet mod k , entonces

$$G(n, \chi) = \bar{\chi}(n) G(1, \chi) \quad \text{si } (n, k) = 1.$$

DEMOSTRACIÓN. Cuando $(n, k) = 1$, los números nr recorren con r un sistema residual completo mod k . Además, $|\chi(n)|^2 = \chi(n) \bar{\chi}(n) = 1$, luego

$$\chi(r) = \bar{\chi}(n) \chi(n) \chi(r) = \bar{\chi}(n) \chi(nr).$$

Por consiguiente la suma que define $G(n, \chi)$ se puede escribir como sigue:

$$\begin{aligned} G(n, \chi) &= \sum_{r \bmod k} \chi(r) e^{2\pi i nr/k} = \bar{\chi}(n) \sum_{r \bmod k} \chi(nr) e^{2\pi i nr/k} \\ &= \bar{\chi}(n) \sum_{m \bmod k} \chi(m) e^{2\pi i im/k} = \bar{\chi}(n) G(1, \chi). \end{aligned}$$

Esto demuestra el teorema. □

Definición. La suma de Gauss $G(n, \chi)$ se dice que es separable si

$$(12) \quad G(n, \chi) = \bar{\chi}(n)G(1, \chi).$$

El teorema 8.9 nos dice que $G(n, \chi)$ es separable si n es primo con el módulo k . Para los enteros n que no son primos con k tenemos el teorema que sigue.

Teorema 8.10 Si χ es un carácter mod k , la suma de Gauss $G(n, \chi)$ es separable para cada n si, y sólo si,

$$G(n, \chi) = 0 \quad \text{si } (n, k) > 1.$$

DEMOSTRACIÓN. La separabilidad se verifica siempre si $(n, k) = 1$. Pero, si $(n, k) > 1$, tenemos $\bar{\chi}(n) = 0$, luego la ecuación (12) se verifica si, y sólo si $G(n, \chi) = 0$. $\square$

El teorema que sigue nos proporciona una consecuencia importante de la separabilidad.

Teorema 8.11 Si $G(n, \chi)$ es separable para cada n , entonces

$$(13) \quad |G(1, \chi)|^2 = k.$$

DEMOSTRACIÓN. Tenemos

$$\begin{aligned} |G(1, \chi)|^2 &= G(1, \chi) \overline{G(1, \chi)} = G(1, \chi) \sum_{m=1}^k \bar{\chi}(m) e^{-2\pi im/k} \\ &= \sum_{m=1}^k G(m, \chi) e^{-2\pi im/k} = \sum_{m=1}^k \sum_{r=1}^k \chi(r) e^{2\pi imr/k} e^{-2\pi im/k} \\ &= \sum_{r=1}^k \chi(r) \sum_{m=1}^k e^{2\pi im(r-1)/k} = k\chi(1) = k, \end{aligned}$$

ya que la última suma respecto a m es una suma geométrica que se anula salvo para $r = 1$. $\square$

8.6 CARACTERES DE DIRICHLET CON SUMAS DE GAUSS NO NULAS

Para cada carácter χ mod k hemos visto que $G(n, \chi)$ es separable si $(n, k) = 1$, y que la separabilidad de $G(n, \chi)$ es equivalente a la anulación de $G(n, \chi)$ para $(n, k) < 1$. Ahora describiremos ciertas propiedades para los caracteres tales que

$G(n, \chi) = 0$ si $(n, k) > 1$. En realidad, es más simple estudiar el conjunto complementario. El teorema que sigue da una condición necesaria para que $G(n, \chi)$ no se anule para $(n, k) > 1$.

Teorema 8.12 *Sea χ un carácter de Dirichlet mod k y supongamos que $G(n, \chi) \neq 0$ para un n con la propiedad $(n, k) > 1$. Entonces existe un divisor d de k , $d < k$, tal que*

$$(14) \quad \chi(a) = 1 \quad \text{si } (a, k) = 1 \text{ y } a \equiv 1 \pmod{d}.$$

DEMOSTRACIÓN. Para el n dado, sea $q = (n, k)$ y sea $d = k/q$. Entonces $d|k$ y, dado que $q > 1$, tenemos $d < k$. Elegimos un a que satisfaga $(a, k) = 1$ y $a \equiv 1 \pmod{d}$. Probaremos que $\chi(a) = 1$.

Puesto que $(a, k) = 1$, en la suma que define $G(n, \chi)$ reemplazamos los índices de sumación m por am y obtenemos

$$\begin{aligned} G(n, \chi) &= \sum_{m \bmod k} \chi(m) e^{2\pi i n m / k} = \sum_{m \bmod k} \chi(am) e^{2\pi i n a m / k} \\ &= \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi i n a m / k}. \end{aligned}$$

Dado que $a \equiv 1 \pmod{d}$ y $d = k/q$, podemos escribir $a = 1 + (bk/q)$ para un cierto entero b , y tenemos

$$\frac{anm}{k} = \frac{nm}{k} + \frac{bknm}{qk} = \frac{nm}{k} + \frac{bnm}{q} \equiv \frac{nm}{k} \pmod{1}$$

ya que $q|n$. Luego $e^{2\pi i n a m / k} = e^{2\pi i n m / k}$ y la suma de $G(n, \chi)$ se transforma en

$$G(n, \chi) = \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi i n m / k} = \chi(a) G(n, \chi).$$

Como $G(n, \chi) \neq 0$ esto implica que $\chi(a) = 1$, tal como habíamos afirmado. $\square$

El teorema que sigue nos lleva a considerar aquellos caracteres $\chi \bmod k$ para los que existe un divisor $d < k$ que satisface (14). Se tratan a continuación.

8.7 MÓDULOS INDUCIDOS Y CARACTERES PRIMITIVOS

Definición de módulo inducido. Sea χ un carácter de Dirichlet mod k y sea d un divisor positivo de k . El número d se llama módulo inducido por χ si se tiene

$$(15) \quad \chi(a) = 1 \quad \text{siempre que } (a, k) = 1 \text{ y } a \equiv 1 \pmod{d}.$$

En otras palabras, d es un módulo inducido si el carácter χ mod k actúa como un carácter módulo d en los representantes de la clase de restos $\hat{1} \pmod{d}$ que son primos con k . Obsérvese que k es a su vez un módulo inducido por χ .

Teorema 8.13. *Sea χ un carácter de Dirichlet mod k . Entonces 1 es un módulo inducido por χ si, y sólo si, $\chi = \chi_1$.*

DEMOSTRACIÓN. Si $\chi = \chi_1$ entonces $\chi(a) = 1$ para todo a primo con k . Pero puesto que cada a satisface $a \equiv 1 \pmod{1}$ el número 1 es un módulo inducido.

Recíprocamente, si 1 es un módulo inducido, entonces $\chi(a) = 1$ siempre que $(a, k) = 1$, luego $\chi = \chi_1$ ya que χ se anula en los números que no son primos con k . $\square$

Para cada carácter de Dirichlet mod k el módulo k es un módulo inducido. Si únicamente existe éste lo llamaremos carácter *primitivo*. Así pues, tenemos:

Definición de caracteres primitivos. Un carácter de Dirichlet χ mod k es primitivo mod k si no existe ningún módulo inducido $d < k$. Con otras palabras, χ es primitivo mod k si, y sólo si, para cada divisor d de k , $0 < d < k$, existe un entero $a \equiv 1 \pmod{d}$, $(a, k) = 1$, tal que $\chi(a) \neq 1$.

Si $k > 1$, el carácter principal χ_1 no es primitivo ya que 1 es un módulo inducido. Ahora vemos que, si el módulo es *primo*, cada carácter no principal es primitivo.

Teorema 8.14 *Cada carácter no principal χ módulo un primo p es un carácter primitivo mod p .*

DEMOSTRACIÓN. Los únicos divisores de p son 1 y p , por lo tanto son los únicos candidatos para inducir módulos. Pero si $\chi \neq \chi_1$ el divisor 1 no es un módulo inducido, por lo tanto χ carece de módulos inducidos $< p$. Luego χ es primitivo. $\square$

Podemos dar nuevos enunciados a los resultados de los teoremas 8.10 a 8.12 utilizando la terminología de los caracteres primitivos.

Teorema 8.15 *Sea χ un carácter primitivo de Dirichlet mod k . Entonces tenemos:*

- (a) $G(n, \chi) = 0$ para cada n con $(n, k) > 1$.
- (b) $G(n, \chi)$ es separable para cada n .
- (c) $|G(1, \chi)|^2 = k$.

DEMOSTRACIÓN. Si $G(n, \chi) \neq 0$ para algún n con $(n, k) > 1$ entonces el teorema 8.12 prueba que χ posee un módulo inducido $d < k$, luego χ no puede ser primitivo. Esto demuestra (a).

La parte (b) se sigue de (a) y del teorema 8.10. La parte (c) se sigue de la parte (b) y del teorema 8.11. □

Nota. El teorema 8.15(b) prueba que la suma de Gauss $G(n, \chi)$ es separable si χ es primitivo. En una sección posterior probaremos el recíproco. Es decir, si $G(n, \chi)$ es separable para cada n , entonces χ es primitivo. (Ver teorema 8.19.)

8.8 OTRAS PROPIEDADES DE LOS MÓDULOS INDUCIDOS

El teorema que sigue se refiere a la acción de χ sobre números que son congruentes módulo un módulo inducido.

Teorema 8.16 *Sea χ un carácter de Dirichlet mod k y supongamos $d|k$, $d > 0$. Entonces d es un módulo inducido por χ si, y sólo si,*

$$(16) \quad \chi(a) = \chi(b) \quad \text{siempre que } (a, k) = (b, k) = 1 \text{ y } a \equiv b \pmod{d}.$$

DEMOSTRACIÓN. Si (16) se verifica entonces d es un módulo inducido ya que podemos elegir $b = 1$ y recurrir a la ecuación (15). Ahora probaremos el recíproco.

Elegimos a y b de forma que $(a, k) = (b, k) = 1$ y $a \equiv b \pmod{d}$. Probaremos que $\chi(a) = \chi(b)$. Sea a' el recíproco de $a \pmod{k}$, $aa' \equiv 1 \pmod{k}$. El recíproco existe porque $(a, k) = 1$. Ahora $aa' \equiv 1 \pmod{d}$ ya que $d|k$. Luego $\chi(aa') = 1$ pues d es un módulo inducido. Pero $aa' \equiv ba' \pmod{d}$ puesto que $a \equiv b \pmod{d}$, luego $\chi(aa') = \chi(ba')$, o sea que

$$\chi(a)\chi(a') = \chi(b)\chi(a').$$

Pero $\chi(a') \neq 0$ ya que $\chi(a)\chi(a') = 1$. Simplificando $\chi(a')$ obtenemos $\chi(a) = \chi(b)$, y ello termina la demostración. □

La ecuación (16) nos dice que χ es periódico mod d sobre los enteros primos con k . Luego χ actúa perfectamente como un carácter mod d . Para explorar más a fondo esta relación merece la pena considerar unos cuantos ejemplos.

EJEMPLO 1 La tabla que sigue describe uno de los caracteres $\chi \bmod 9$.

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	-1	0	1	-1	0	1	-1	0

Observemos que esta tabla es periódica módulo 3, luego 3 es un módulo inducido por χ . En efecto, χ actúa como el siguiente carácter ψ módulo 3:

n	1	2	3
$\psi(n)$	1	-1	0

Como $\chi(n) = \psi(n)$ para todo n , llamamos a χ *extensión* de ψ . Es claro que si χ es una extensión de un carácter ψ módulo d , entonces d es un módulo inducido por χ .

EJEMPLO 2 Ahora examinamos uno de los caracteres χ módulo 6:

n	1	2	3	4	5	6
$\chi(n)$	1	0	0	0	-1	0

En este caso el número 3 es un módulo inducido porque $\chi(n) = 1$ para todo $n \equiv 1 \pmod{3}$ con $(n, 6) = 1$. (Sólo existe un n como éste, a saber, $n = 1$.) Sin embargo, χ *no* es una extensión de un carácter ψ módulo 3, porque los únicos caracteres módulo 3 son los caracteres principales ψ_1 , dados por la tabla:

n	1	2	3
$\psi_1(n)$	1	1	0

y el carácter ψ presentado en el ejemplo 1. Puesto que $\chi(2) = 0$ no puede ser ni una extensión de ψ ni de ψ_1 .

Estos ejemplos vierten cierta luz sobre el próximo teorema.

Teorema 8.17 Sea χ un carácter de Dirichlet módulo k y sea $d|k$, $d < k$. Las afirmaciones que siguen son equivalentes:

- (a) d es un módulo inducido por χ .
- (b) Existe un carácter ψ módulo d tal que

$$(17) \quad \chi(n) = \psi(n)\chi_1(n) \quad \text{para todo } n,$$

en donde χ_1 es el carácter principal módulo k .

DEMOSTRACIÓN. Suponemos que (b) se verifica. Elegimos n que satisfaga $(n, k) = 1$, $n \equiv 1 \pmod{d}$. Entonces $\chi_1(n) = \psi(n) = 1$, luego $\chi(n) = 1$ y por lo tanto d es un módulo inducido. Entonces (b) implica (a).

Ahora suponemos que (a) se verifica. Mostraremos un carácter ψ módulo d para el cual (17) se verifica. Definimos $\psi(n)$ como sigue: Si $(n, d) > 1$, sea $\psi(n) = 0$. En este caso tenemos también $(n, k) > 1$, luego (17) se verifica porque ambos miembros son cero.

Ahora suponemos que $(n, d) = 1$. Entonces existe un entero m tal que $m \equiv n \pmod{d}$, $(m, k) = 1$. Esto se puede demostrar directamente utilizando el teorema de Dirichlet. La progresión aritmética $xd + n$ contiene una infinidad de primos. Elegimos uno que no divida a k y lo llamamos m . Sin embargo el resultado no es tan profundo; la existencia del número m se puede establecer fácilmente sin utilizar el teorema de Dirichlet. (Ver ejercicio 8.4 para otra demostración.) Habiendo elegido m , que es único módulo d , definimos

$$\psi(n) = \chi(m).$$

El número $\psi(n)$ está bien definido porque χ toma los mismos valores en los números que son congruentes módulo d y primos con k .

El lector puede comprobar fácilmente que χ es, verdaderamente, un carácter mod d . Veremos que la ecuación (17) se verifica para todo n .

Si $(n, k) = 1$ entonces $(n, d) = 1$ luego $\psi(n) = \chi(m)$ para algún $m \equiv n \pmod{d}$. Luego, por el teorema 8.16,

$$\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_1(n)$$

ya que $\chi_1(n) = 1$.

Si $(n, k) > 1$, entonces $\chi(n) = \chi_1(n) = 0$ y ambos miembros de (17) son 0. Luego, (17) vale para todo n . □

8.9 EL CONDUCTOR DE UN CARÁCTER

Definición. Sea χ un carácter de Dirichlet mod k . El menor módulo inducido d por χ se llama conductor de χ .

Teorema 8.18 *Cada carácter de Dirichlet χ mod k se puede expresar como un producto,*

$$(18) \quad \chi(n) = \psi(n)\chi_1(n) \quad \text{para todo } n,$$

en donde χ_1 es el carácter principal mod k y ψ es un carácter primitivo módulo el conductor de ψ .

DEMOSTRACIÓN. Sea d el conductor de χ . Por el teorema 8.17 sabemos que χ se puede expresar como un producto de la forma (18), en donde ψ es un carácter mod d . Probaremos que ψ es primitivo mod d .

Suponemos que ψ no es primitivo mod d y obtenemos una contradicción. Si ψ no es primitivo mod d existe un divisor q de d , $q < d$, que es un módulo inducido por ψ . Probaremos que este q , que divide a k , también es un módulo inducido por χ , en contradicción con el hecho de que d es el menor módulo inducido por χ .

Elegimos $n \equiv 1 \pmod{q}$, $(n, k) = 1$. Entonces

$$\chi(n) = \psi(n)\chi_1(n) = \psi(n) = 1$$

porque q es un módulo inducido por ψ . Luego q también es un módulo inducido por χ y obtenemos una contradicción. $\square$

8.10 CARACTERES PRIMITIVOS Y SUMAS DE GAUSS SEPARABLES

Como aplicación de los teoremas anteriores damos la siguiente descripción alternativa de carácter primitivo.

Teorema 8.19 *Sea χ un carácter mod k . Entonces χ es primitivo mod k si, y sólo si, la suma de Gauss*

$$G(n, \chi) = \sum_{m \bmod k} \chi(m) e^{2\pi i mn/k}$$

es separable para cada n .

DEMOSTRACIÓN. Si χ es primitivo, entonces $G(n, \chi)$ es separable por el teorema 8.15(b). Ahora probaremos el recíproco.

En virtud de los teoremas 8.9 y 8.10 es suficiente probar que, si χ no es primitivo mod k , entonces para un r que satisfaga $(r, k) > 1$ tenemos $G(r, \chi) \neq 0$. Suponemos, entonces, que χ no es primitivo mod k . Ello implica $k > 1$. Entonces χ tiene un conductor $d < k$. Sea $r = k/d$. Entonces $(r, k) > 1$ y probaremos que $G(r, \chi) \neq 0$ para este r . Por el teorema 8.18 existe un carácter primitivo ψ mod d tal que $\chi(n) = \psi(n)\chi_1(n)$ para todo n . Por lo tanto podemos escribir

$$\begin{aligned} G(r, \chi) &= \sum_{m \bmod k} \psi(m)\chi_1(m)e^{2\pi i r m/k} = \sum_{\substack{m \bmod k \\ (m, k) = 1}} \psi(m)e^{2\pi i r m/k} \\ &= \sum_{\substack{m \bmod k \\ (m, k) = 1}} \psi(m)e^{2\pi i m/d} = \frac{\varphi(k)}{\varphi(d)} \sum_{\substack{m \bmod d \\ (m, d) = 1}} \psi(m)e^{2\pi i m/d}, \end{aligned}$$

en donde en el último paso hemos utilizado el teorema 5.33(a). Por consiguiente tenemos

$$G(r, \chi) = \frac{\varphi(k)}{\varphi(d)} G(1, \psi).$$

Pero $|G(1, \psi)|^2 = d$ por el teorema 8.15 (ya que ψ es primitivo mod d) y por lo tanto $G(r, \chi) \neq 0$. Esto termina la demostración. $\square$

8.11 LA SERIE FINITA DE FOURIER DE LOS CARACTERES DE DIRICHLET

Puesto que cada carácter de Dirichlet χ mod k es periódico mod k admite un desarrollo finito de Fourier

$$(19) \quad \chi(m) = \sum_{n=1}^k a_k(n) e^{2\pi i m n/k},$$

y el teorema 8.4 nos dice que sus coeficientes vienen dados por la fórmula

$$a_k(n) = \frac{1}{k} \sum_{m=1}^k \chi(m) e^{-2\pi i m n/k}.$$

La suma de la derecha es una suma de Gauss $G(-n, \chi)$ luego tenemos

$$(20) \quad a_k(n) = \frac{1}{k} G(-n, \chi).$$

Cuando χ es primitivo, el desarrollo de Fourier (19) se puede expresar como sigue:

Teorema 8.20 *El desarrollo finito de Fourier de un carácter de Dirichlet primitivo mod k tiene la forma*

$$(21) \quad \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^k \bar{\chi}(n) e^{-2\pi i m n/k}$$

en donde

$$(22) \quad \tau_k(\chi) = \frac{G(1, \chi)}{\sqrt{k}} = \frac{1}{\sqrt{k}} \sum_{m=1}^k \chi(m) e^{2\pi i m/k}.$$

Los números $\tau_k(\chi)$ tienen valor absoluto 1.

DEMOSTRACIÓN. Como χ es primitivo tenemos $G(-n, \chi) = \bar{\chi}(-n)G(1, \chi)$ y (20) implica $a_k(n) = \bar{\chi}(-n)G(1, \chi)/k$. Por consiguiente (19) se puede escribir

$$\chi(m) = \frac{G(1, \chi)}{k} \sum_{n=1}^k \bar{\chi}(-n) e^{2\pi i m n/k} = \frac{G(1, \chi)}{k} \sum_{n=1}^k \bar{\chi}(n) e^{-2\pi i m n/k},$$

que es lo mismo que (21). El teorema 8.11 prueba que los números $\tau_k(\chi)$ tienen valor absoluto 1. $\square$

8.12 DESIGUALDAD DE PÓLYA PARA SUMAS PARCIALES DE CARACTERES PRIMITIVOS

La demostración del teorema de Dirichlet dada en el capítulo 7 utiliza la relación

$$\left| \sum_{m \leq x} \chi(m) \right| \leq \varphi(k)$$

válida para todo carácter de Dirichlet χ mod k y cada real $x \geq 1$. No es posible mejorar este resultado cuando $\chi = \chi_1$ puesto que $\sum_{m=1}^k \chi_1(m) = \chi(k)$. Sin embargo Pólya demostró que cuando χ es un carácter primitivo, la desigualdad se puede mejorar considerablemente.

Teorema 8.21 Desigualdad de Pólya. Si χ es un carácter primitivo mod k , entonces para todo $x \geq 1$ tenemos

$$(23) \quad \left| \sum_{m \leq x} \chi(m) \right| < \sqrt{k} \log k.$$

DEMOSTRACIÓN. Expresemos $\chi(m)$ por medio de su desarrollo finito de Fourier, tal como se da en el teorema 8.20

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^k \tilde{\chi}(n) e^{-2\pi i m n/k},$$

y sumemos para todo $m \leq x$ a fin de obtener

$$\sum_{m \leq x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \tilde{\chi}(n) \sum_{m \leq x} e^{-2\pi i m n/k}$$

ya que $\chi(k) = 0$. Tomando valores absolutos y multiplicando por $\sqrt{k}$ obtenemos

$$(24) \quad \sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq \sum_{n=1}^{k-1} \left| \sum_{m \leq x} e^{-2\pi i m n/k} \right| = \sum_{n=1}^{k-1} |f(n)|,$$

en donde

$$f(n) = \sum_{m \leq x} e^{-2\pi i m n/k}.$$

Ahora

$$f(k-n) = \sum_{m \leq x} e^{-2\pi i m (k-n)/k} = \sum_{m \leq x} e^{2\pi i m n/k} = \overline{f(n)}$$

luego

$|f(k-n)| = |f(n)|$. Por lo tanto (24) se puede escribir en la forma

$$(25) \quad \sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq 2 \sum_{n \leq k/2} |f(n)|.$$

Ahora bien $f(n)$ es una suma geométrica de la forma

$$f(n) = \sum_{m=1}^r y^m$$

en donde $r = [x]$ e $y = e^{-2}$. Aquí $y \neq 1$ ya que $1 \leq n \leq k-1$. Si escribimos $z = e^{-\pi i n/k}$, tenemos $y = z^2$ y $z^2 \neq 1$ ya que $n \leq k/2$. Luego tenemos

$$f(n) = y \frac{y^r - 1}{y - 1} = z^2 \frac{z^{2r} - 1}{z^2 - 1} = z^{r+1} \frac{z^r - z^{-r}}{z - z^{-1}}$$

o sea

$$(26) \quad |f(n)| = \left| \frac{z^r - z^{-r}}{z - z^{-1}} \right| = \left| \frac{e^{-\pi i r n/k} - e^{\pi i r n/k}}{e^{-\pi i n/k} - e^{\pi i n/k}} \right| = \frac{\left| \frac{\sin \frac{\pi r n}{k}}{k} \right|}{\left| \frac{\sin \frac{\pi n}{k}}{k} \right|} \leq \frac{1}{\sin \frac{\pi n}{k}}.$$

Ahora utilizamos la desigualdad $\sin t \geq 2t/\pi$, válida para $0 \leq t \leq \pi/2$, con $t = \pi n/k$ para obtener

$$|f(n)| \leq \frac{1}{2 \frac{\pi n}{k}} = \frac{k}{2n}.$$

Luego (25) se transforma en

$$\sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq k \sum_{n \leq k/2} \frac{1}{n} < k \log k,$$

que prueba (23).

Nota. En un capítulo posterior demostraremos que la desigualdad de Pólya se puede extender a todo carácter no principal. Para caracteres no primitivos toma la forma

$$\sum_{m \leq x} \chi(m) = O(\sqrt{k} \log k).$$

(Ver teorema 13.15).

Ejercicios del capítulo 8

1. Sea $x = e^{2\pi i/n}$ y probar que

$$\sum_{k=1}^{n-1} kx^k = \frac{n}{x-1}.$$

2. Sea $((x)) = x - [x] - \frac{1}{2}$ si x no es un entero, y sea $((x)) = 0$ en otro caso. Obsérvese que $((x))$ es una función periódica de x de período 1. Si k y n son enteros, con $n > 0$, probar que

$$\left(\left(\frac{k}{n} \right) \right) = -\frac{1}{2n} \sum_{m=1}^{n-1} \cot \frac{\pi m}{n} \operatorname{sen} \frac{2\pi km}{n}.$$

3. Sea $c_k(m)$ la suma de Ramanujan y sea $M(x) = \sum_{n \leq x} \mu(n)$, las sumas parciales de la función de Möbius.

- (a) Probar que

$$\sum_{k=1}^n c_k(m) = \sum_{d|m} dM\left(\frac{n}{d}\right).$$

En particular, cuando $n = m$, tenemos

$$\sum_{k=1}^m c_k(m) = \sum_{d|m} dM\left(\frac{m}{d}\right).$$

- (b) Utilizar (a) para deducir que

$$M(m) = m \sum_{d|m} \frac{\mu(m/d)}{d} \sum_{k=1}^d c_k(d).$$

- (c) Probar que

$$\sum_{m=1}^n c_k(m) = \sum_{d|k} d\mu\left(\frac{k}{d}\right) \left[\frac{n}{d} \right].$$

4. Sean n, a, d enteros dados con $(a, d) = 1$. Sea $m = a + qd$, en donde q es el producto (que puede ser vacío) de todos los primos que dividen a n , pero no dividen a a . Probar que

$$m \equiv a \pmod{d} \quad \text{y} \quad (m, n) = 1.$$

5. Probar que existe un carácter primitivo no real $\chi \pmod{k}$ si $k = 2m$, en donde m es impar.
 6. Sea χ un carácter $\pmod{k}$. Si k_1 y k_2 son módulos inducidos por χ , probar que su mcd (k_1, k_2) también lo es.
 7. Probar que el conductor de χ divide a cada uno de los módulos inducidos para χ .

En los ejercicios del 8 al 12 suponemos que $k = k_1 k_2 \dots k_r$, en donde los enteros positivos k_i son primos dos a dos: $(k_i, k_j) = 1$ si $i \neq j$.

8. (a) Dado un entero a , probar que existe un entero a_i tal que

$$a_i \equiv a \pmod{k_i} \quad \text{y} \quad a_i \equiv 1 \pmod{k_j} \quad \text{para todo } j \neq i.$$

- (b) Sea χ un carácter mod k . Definimos χ_i por la ecuación

$$\chi_i(a) = \chi(a_i),$$

en donde a_i es el entero de la parte (a). Probar que χ_i es un carácter mod k_i .

9. Probar que cada carácter χ mod k se descompone, de forma única, en un producto de la forma $\chi = \chi_1 \chi_2 \dots \chi_r$, en donde χ_i es un carácter mod k_i .
 10. $f(\chi)$ designa el conductor de χ . Si χ admite la descomposición del ejercicio 9, probar que $f(\chi) = f(\chi_1) \dots f(\chi_r)$.
 11. Si χ posee la descomposición del ejercicio 9, probar que, para cada entero a , tenemos

$$G(a, \chi) = \prod_{i=1}^r \chi_i\left(\frac{k}{k_i}\right) G(a_i, \chi_i),$$

en donde a_i es el entero del ejercicio 8.

12. Si χ admite la descomposición del ejercicio 9, probar que χ es primitivo mod k si, y sólo si, cada χ_i es primitivo mod k_i . [Indicación: teorema 8.19.]
 13. Sea χ un carácter primitivo mod k . Probar que, si $N < M$, tenemos

$$\left| \sum_{m=N+1}^M \frac{\chi(m)}{m} \right| < \frac{2}{N+1} \sqrt{k} \log k.$$

14. Este ejercicio esboza una ligera mejora en la desigualdad de Pólya. Considerar la demostración del teorema 8.21. A partir de la desigualdad (26) escribir

$$\sum_{n \leq k/2} |f(n)| \leq \sum_{n \leq k/2} \frac{1}{\frac{\pi n}{k}} < \frac{1}{\frac{\pi}{k}} + \int_1^{k/2} \frac{dt}{\frac{\pi t}{k}}.$$

Probar que la integral es menor que $-(k/\pi) \log(\sin(\pi/2k))$ y deducir que

$$\left| \sum_{n \leq x} \chi(n) \right| < \sqrt{k} + \frac{2}{\pi} \sqrt{k} \log k.$$

Esta mejora en la desigualdad de Pólya resulta del factor $2/\pi$ en el término principal.

15. La suma de Kloosterman $K(m, n; k)$ se define como sigue:

$$K(m, n; k) = \sum_{\substack{h \bmod k \\ (h, k) = 1}} e^{2\pi i(mh + nh')/k}$$

en donde h' es el inverso de h mod k . Cuando $k|n$ se reduce a la suma de Ramanujan $c_k(m)$. Obtener las siguientes propiedades de las sumas de Kloosterman:

- (a) $K(m, n; k) = K(n, m; k)$.
 (b) $K(m, n; k) = K(1, mn, k)$ siempre que $(m, k) = 1$.
 (c) Dados enteros n, k_1, k_2 con $(k_1, k_2) = 1$, probar que existen enteros n_1 y n_2 tales que

$$n \equiv n_1 k_2^2 + n_2 k_1^2 \pmod{k_1 k_2},$$

y que, para estos enteros, tenemos

$$K(m, n; k_1 k_2) = K(m, n_1; k_1) K(m, n_2; k_2).$$

Este resultado reduce el estudio de las sumas de Kloosterman al caso especial $K(m, n; p^\alpha)$, en donde p es primo.

16. Si n y k son enteros, $n > 0$, la suma

$$G(k; n) = \sum_{r=1}^n e^{2\pi i k r^2 / n}$$

se llama suma cuadrática de Gauss. Obtener las siguientes propiedades de las sumas cuadráticas de Gauss:

- (a) $G(k; mn) = G(km; n)G(kn; m)$ siempre que $(m, n) = 1$. Este hecho reduce el estudio de las sumas de Gauss al caso especial $G(k; p^\alpha)$, en donde p es primo.
 (b) Sea p un primo impar, $p \nmid k$, $\alpha \geq 2$. Probar que $G(k; p^\alpha) = pG(k; p^{\alpha-2})$ y deducir que

$$G(k; p^\alpha) = \begin{cases} p^{\alpha/2} & \text{si } \alpha \text{ es par;} \\ p^{(\alpha-1)/2} G(k; p) & \text{si } \alpha \text{ es impar} \end{cases}$$

En el capítulo siguiente desarrollaremos otras propiedades de la suma de Gauss $G(k; p)$ y probaremos que $G(k; p)$ es la misma que la suma de Gauss $G(k, \chi)$ asociada con cierto carácter de Dirichlet $\chi \pmod{p}$. (Ver ejercicio 9.9.)

Capítulo 9

Restos cuadráticos y ley de reciprocidad cuadrática

9.1 RESTOS CUADRÁTICOS

Como indicábamos en el capítulo 5, el problema de resolver una congruencia polinómica

$$f(x) \equiv 0 \pmod{m}$$

se puede reducir a congruencias polinómicas con módulos primos junto con un sistema de congruencias lineales. En este capítulo trataremos las congruencias cuadráticas de la forma.

$$(1) \quad x^2 \equiv n \pmod{p}$$

en donde p es un primo impar y $n \not\equiv 0 \pmod{p}$. Puesto que el módulo es primo sabemos que (1) tiene a lo sumo dos soluciones. Sin embargo, si x es una solución también lo es $-x$, luego el número de soluciones es 0 o 2.

Definición. Si la congruencia (1) tiene una solución diremos que n es un resto cuadrático mod p y escribiremos nRp . Si (1) carece de solución diremos que n no es un resto cuadrático —o bien que es un no resto cuadrático— y escribiremos $n\bar{R}p$.

Dos problemas básicos dominan la teoría de los restos cuadráticos:

1. Dado un primo p , determinar cuáles son los n que son restos cuadráticos mod p y cuáles no son restos cuadráticos mod p .
2. Dado n , determinar aquellos primos p para los que n es un resto cuadrático mod p y aquellos para los que n no es un resto cuadrático mod p .

Empezaremos con algunos métodos conducentes a resolver el problema 1.

EJEMPLO Para buscar los restos cuadráticos módulo 11, elevamos al cuadrado los números 1, 2, ..., 10 y reducimos mod 11. Obtenemos

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 5, \quad 5^2 \equiv 3 \pmod{11}.$$

Es suficiente elevar al cuadrado la primera mitad de los números ya que

$$6^2 \equiv (-5)^2 \equiv 3, \quad 7^2 \equiv (-4)^2 \equiv 5, \dots, 10^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

En consecuencia, los restos cuadráticos mod 11 son 1, 3, 4, 5, 9, y los no restos son 2, 6, 7, 8, 10.

Este ejemplo ilustra el siguiente teorema.

Teorema 9.1 *Sea p un primo impar. Entonces cada sistema residual reducido mod p contiene exactamente $(p-1)/2$ restos cuadráticos y exactamente $(p-1)/2$ restos no cuadráticos mod p . Los restos cuadráticos pertenecen a las clases residuales que contienen a los números*

$$(2) \quad 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

DEMOSTRACIÓN. Observemos en primer lugar que los números de (2) son distintos mod p . En efecto, si $x^2 \equiv y^2 \pmod{p}$ con $1 \leq x \leq (p-1)/2$ y $1 \leq y \leq (p-1)/2$, entonces

$$(x-y)(x+y) \equiv 0 \pmod{p}.$$

Pero $1 < x+y < p$, luego $x-y \equiv 0 \pmod{p}$, y por tanto $x=y$. Como

$$(p-k)^2 \equiv k^2 \pmod{p},$$

cada resto cuadrático es congruente mod p con uno exactamente de los números de (2). Esto termina la demostración. $\square$

La breve tabla de los restos cuadráticos R y de los no restos $\bar{R}$ que se expone a continuación se obtuvo con la ayuda del teorema 9.1.

	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$
R :	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12
$\bar{R}$:	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

9.2 EL SÍMBOLO DE LEGENDRE Y SUS PROPIEDADES

Definición. Sea p un primo impar. Si $n \not\equiv 0 \pmod{p}$ definimos el símbolo de Legendre $(n|p)$ como sigue:

$$(n|p) = \begin{cases} +1 & \text{si } nRp, \\ -1 & \text{si } n\bar{R}p. \end{cases}$$

Si $n \equiv 0 \pmod{p}$ definimos $(n|p) = 0$.

EJEMPLOS $(1|p) = 1$, $(m^2|p) = 1$, $(7|11) = -1$, $(22|11) = 0$.

Nota. Algunos autores escriben $\left(\frac{n}{p}\right)$ en vez de $(n|p)$.

Es claro que $(m|p) = (n|p)$ siempre que $m \equiv n \pmod{p}$, luego $(n|p)$ es una función periódica de n con período p .

El teorema débil de Fermat nos dice que $n^{p-1} \equiv 1 \pmod{p}$ si $p \nmid n$. Como

$$n^{p-1} - 1 = (n^{(p-1)/2} - 1)(n^{(p-1)/2} + 1)$$

obtenemos que $n^{(p-1)/2} \equiv \pm 1 \pmod{p}$. El teorema que sigue nos dice que obtenemos $+1$ si nRp y -1 si $n\bar{R}p$.

Teorema 9.2 Criterio de Euler. Sea p un número primo impar. Entonces, para todo n , tenemos

$$(n|p) \equiv n^{(p-1)/2} \pmod{p}.$$

DEMOSTRACIÓN. Si $n \equiv 0 \pmod{p}$ el resultado es trivial ya que ambos miembros son congruentes con $0 \pmod{p}$. Ahora suponemos que $(n|p) = 1$. Entonces existe un x tal que $x^2 \equiv n \pmod{p}$ y por tanto

$$n^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 = (n|p) \pmod{p}.$$

Esto prueba el teorema si $(n|p) = 1$.

Ahora suponemos que $(n|p) = -1$ y consideramos el polinomio

$$f(x) = x^{(p-1)/2} - 1.$$

Como el grado de $f(x)$ es $(p-1)/2$ la congruencia

$$f(x) \equiv 0 \pmod{p}$$

tiene, a lo sumo $(p-1)/2$ soluciones. Pero los $(p-1)/2$ restos cuadráticos mod p son soluciones por lo que no son soluciones los no restos. Luego

$$n^{(p-1)/2} \not\equiv 1 \pmod{p} \quad \text{si} \quad (n|p) = -1.$$

Pero $n^{(p-1)/2} \equiv \pm 1 \pmod{p}$, por tanto $n^{(p-1)/2} \equiv -1 \equiv (n|p) \pmod{p}$. Esto termina la demostración. $\square$

Teorema 9.3 *El símbolo de Legendre $(n|p)$ es una función completamente multiplicativa de n .*

DEMOSTRACIÓN. Si $p|m$ o $p|n$ entonces $p|mn$ luego $(mn|p) = 0$ y es $(m|p) = 0$ o bien $(n|p) = 0$. Por consiguiente $(mn|p) = (m|p)(n|p)$ si $p \nmid m$ o $p \nmid n$.

Si $p \nmid m$ y $p \nmid n$ entonces $p \nmid mn$ y tenemos

$$(mn|p) \equiv (mn)^{(p-1)/2} = m^{(p-1)/2} n^{(p-1)/2} \equiv (m|p)(n|p) \pmod{p}.$$

Pero cada uno de los $(mn|p)$, $(m|p)$ y $(n|p)$ es 1 ó -1 luego la diferencia

$$(mn|p) - (m|p)(n|p)$$

es 0, 2 ó -2. Puesto que esta diferencia es divisible por p debe ser 0. $\square$

Nota. Como $(n|p)$ es una función completamente multiplicativa de n , periódica de período p y que se anula cuando $p|n$, tenemos que $(n|p) = \chi(n)$, en donde χ es uno de los caracteres de Dirichlet módulo p . El símbolo de Legendre se llama el *carácter cuadrático* mod p .

9.3 CÁLCULO DE $(-1|p)$ Y $(2|p)$

Teorema 9.4 Para cada primo impar p tenemos

$$(-1|p) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4}, \\ -1 & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

DEMOSTRACIÓN. Por el criterio de Euler tenemos $(-1|p) \equiv (-1)^{(p-1)/2} \pmod{p}$. Dado que cada miembro de esta congruencia es 1 o -1 , ambos miembros son iguales. $\square$

Teorema 9.5 Para cada primo impar p tenemos

$$(2|p) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$

DEMOSTRACIÓN. Consideremos las $(p-1)/2$ congruencias siguientes:

$$\begin{aligned} p-1 &\equiv 1(-1)^1 && \pmod{p} \\ 2 &\equiv 2(-1)^2 && \pmod{p} \\ p-3 &\equiv 3(-1)^3 && \pmod{p} \\ 4 &\equiv 4(-1)^4 && \pmod{p} \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} && \pmod{p}, \end{aligned}$$

en donde r es $p - (p-1)/2$ o $(p-1)/2$. Multiplicamos estas congruencias y observamos que cada entero de la izquierda es par. Obtenemos

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)! (-1)^{1+2+\cdots+(p-1)/2} \pmod{p}.$$

Esto nos da

$$2^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (-1)^{(p^2-1)/8} \pmod{p}.$$

Como $((p-1)/2)! \not\equiv 0 \pmod{p}$ tenemos

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod{p}.$$

Por el criterio de Euler tenemos $2^{(p-1)/2} \equiv (2|p) \pmod{p}$, y como cada uno de estos miembros es 1 o -1, ambos miembros son iguales. Esto termina la demostración. $\square$

9.4 LEMA DE GAUSS

Aunque el criterio de Euler nos proporciona un método directo para calcular $(n|p)$, el cálculo puede resultar prohibitivo para n grande ya que requiere elevar n a la potencia $(p-1)/2$. Gauss halló otro criterio que implica un cálculo más simple.

Teorema 9.6 Lema de Gauss. *Suponemos $n \not\equiv 0 \pmod{p}$ y consideramos el mínimo resto positivo mod p de los siguientes $(p-1)/2$ múltiplos de n :*

$$(3) \quad n, 2n, 3n, \dots, \frac{p-1}{2}n.$$

Si m designa el número de restos que exceden a $p/2$, entonces

$$(n|p) = (-1)^m.$$

DEMOSTRACIÓN. Los números de (3) son incongruentes mod p . Consideramos sus mínimos restos positivos y los distribuimos en dos conjuntos disjuntos A y B , según que los restos sean $< p/2$ o $> p/2$. Sean

$$A = \{a_1, a_2, \dots, a_k\}$$

en donde cada $a_i \equiv tn \pmod{p}$ para algún $t \leq (p-1)/2$ y $0 < a_i < p/2$; y

$$B = \{b_1, b_2, \dots, b_m\}$$

en donde $b_i \equiv sn \pmod{p}$ para algún $s \leq (p-1)/2$ y $p/2 < b_i < p$. Vemos que $m + k = (p-1)/2$ pues A y B son disjuntos. El número m de elementos de B es significativo en este teorema. Formamos un nuevo conjunto C de m elementos restando cada b_i de p . Entonces

$$C = \{c_1, c_2, \dots, c_m\}, \text{ en donde } c_i = p - b_i.$$

Ahora $0 < c_i < p/2$, luego los elementos de C pertenecen al mismo intervalo que los elementos de A . A continuación vemos que los conjuntos A y C son disjuntos.

Suponemos que $c_i = a_j$ para algún i y j . Entonces $p - b_i = a_j$, o $a_j + b_i \equiv 0 \pmod{p}$. Por consiguiente

$$tn + sn = (t + s)n \equiv 0 \pmod{p}$$

para ciertos s y t con $1 \leq t < p/2$, $1 \leq s < p/2$. Pero esto es imposible ya que $p \nmid n$ y $0 < s + t < p$. Por consiguiente A y C son disjuntos, luego su unión $A \cup C$ contiene $m + k = (p - 1)/2$ enteros en el intervalo $[1, (p - 1)/2]$. Luego

$$A \cup C := \{a_1, a_2, \dots, a_k, c_1, c_2, \dots, c_m\} = \left\{1, 2, \dots, \frac{p-1}{2}\right\}.$$

Formamos ahora el producto de todos los elementos de $A \cup C$ a fin de obtener

$$a_1 a_2 \cdots a_k c_1 c_2 \cdots c_m = \left(\frac{p-1}{2}\right)!.$$

Puesto que $c_i = p - b_i$ esto nos da

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= a_1 a_2 \cdots a_k (p - b_1)(p - b_2) \cdots (p - b_m) \\ &\equiv (-1)^m a_1 a_2 \cdots a_k b_1 b_2 \cdots b_m \pmod{p} \\ &\equiv (-1)^m n(2n)(3n) \cdots \left(\frac{p-1}{2}n\right) \pmod{p} \\ &\equiv (-1)^m n^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Simplificando el factorial obtenemos

$$n^{(p-1)/2} \equiv (-1)^m \pmod{p}.$$

El criterio de Euler demuestra que $(-1)^m \equiv (n|p) \pmod{p}$ luego $(-1)^m = (n|p)$ y queda establecida la demostración del lema de Gauss. $\square$

En la práctica para utilizar el lema de Gauss no es necesario conocer el valor exacto de m , sino únicamente su paridad, esto es, saber si m es par o impar. El teorema que sigue nos da un método relativamente simple para determinar la paridad de m .

Teorema 9.7 Sea m el número definido en el lema de Gauss. Entonces

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right] + (n-1) \frac{p^2-1}{8} \pmod{2}.$$

En particular, si n es impar tenemos

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right] \pmod{2}.$$

DEMOSTRACIÓN. Recordemos que m es el número mínimo de restos positivos de los números

$$n, 2n, 3n, \dots, \frac{p-1}{2}n$$

que exceden a $p/2$. Tomemos un número típico, tal como tn , dividámoslo por p y examinemos el tamaño de su resto. Tenemos

$$\frac{tn}{p} = \left[\frac{tn}{p} \right] + \left\{ \frac{tn}{p} \right\}, \text{ en donde } 0 < \left\{ \frac{tn}{p} \right\} < 1,$$

luego

$$tn = p \left[\frac{tn}{p} \right] + p \left\{ \frac{tn}{p} \right\} = p \left[\frac{tn}{p} \right] + r_t,$$

en donde $0 < r_t < p$. El número $r_t = tn - p[tn/p]$ es el mínimo resto positivo de tn módulo p . Si nos referimos de nuevo a los conjuntos A y B utilizados en la demostración del lema de Gauss tenemos

$$\{r_1, r_2, \dots, r_{(p-1)/2}\} = \{a_1, a_2, \dots, a_k, b_1, \dots, b_m\}.$$

Recordemos asimismo que

$$\left\{ 1, 2, \dots, \frac{p-1}{2} \right\} = \{a_1, a_2, \dots, a_k, c_1, \dots, c_m\}$$

en donde cada $c_i = p - b_i$. Ahora calculamos las sumas de los elementos de estos conjuntos y obtenemos las dos ecuaciones

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^k a_i + \sum_{j=1}^m b_j$$

y

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^k a_i + \sum_{j=1}^m c_j = \sum_{i=1}^k a_i + mp - \sum_{j=1}^m b_j.$$

En la primera ecuación reemplazamos r_t por su definición y obtenemos

$$\sum_{i=1}^k a_i + \sum_{j=1}^m b_j = n \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right].$$

La segunda ecuación es

$$mp + \sum_{i=1}^k a_i - \sum_{j=1}^m b_j = \sum_{t=1}^{(p-1)/2} t.$$

Sumando ésta a la ecuación anterior obtenemos

$$\begin{aligned} mp + 2 \sum_{i=1}^k a_i &= (n+1) \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right] \\ &= (n+1) \frac{p^2-1}{8} - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right]. \end{aligned}$$

Reducimos ahora este resultado módulo 2, observando que $n+1 \equiv n-1 \pmod{2}$ y $p \equiv 1 \pmod{2}$, y obtenemos

$$m \equiv (n-1) \frac{p^2-1}{8} + \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p} \right] \pmod{2},$$

que termina la demostración. □

9.5 LA LEY DE RECIPROCIDAD CUADRÁTICA

Tanto el criterio de Euler como el lema de Gauss dan un método poderoso, si bien largo, para resolver el primer problema básico de la teoría de los restos cuadráticos. El segundo problema es mucho más difícil. Su solución depende de un teorema notable conocido como *ley de reciprocidad cuadrática*, establecido primeramente de forma complicada por Euler en el período 1744-1746, y redescu-

bierto en 1785 por Legendre que dio una demostración parcial. Gauss, por su cuenta, descubrió la ley de reciprocidad a la edad de dieciocho años y un año más tarde en 1796 dio la primera demostración completa.

La ley de reciprocidad cuadrática establece que, si p y q son primos impares distintos, entonces $(p|q) = (q|p)$ salvo para $p \equiv q \equiv 3 \pmod{4}$, en cuyo caso $(p|q) = -(q|p)$. El teorema se establece usualmente en la siguiente forma simétrica dada por Legendre.

Teorema 9.8 Ley de reciprocidad cuadrática. Si p y q son primos impares distintos, entonces

$$(4) \quad (p|q)(q|p) = (-1)^{(p-1)(q-1)/4}.$$

DEMOSTRACIÓN. Por el lema de Gauss y el teorema 9.7 tenemos

$$(q|p) = (-1)^m$$

en donde

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p} \right] \pmod{2}.$$

Análogamente

$$(p|q) = (-1)^n$$

en donde

$$n \equiv \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q} \right] \pmod{2}.$$

Luego $(p|q)(q|p) = (-1)^{m+n}$, y (4) sigue inmediatamente de la identidad

$$(5) \quad \sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p} \right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q} \right] = \frac{p-1}{2} \frac{q-1}{2}.$$

Para probar (5) consideramos la función

$$f(x, y) = qx - py.$$

Si x e y son enteros no nulos, entonces $f(x, y)$ es un entero no nulo. Sin embargo, dado que x toma los valores $1, 2, \dots, (p-1)/2$ e y toma los valores $1, 2, \dots, (q-1)/2$, entonces $f(x, y)$ toma

$$\frac{p-1}{2} \frac{q-1}{2}$$

valores, distintos dos a dos ya que

$$f(x, y) - f(x', y') = f(x - x', y - y') \neq 0.$$

Ahora contamos el número de valores de $f(x, y)$ positivos y el número de los que son negativos.

Para cada x fijo tenemos $f(x, y) > 0$ si, y sólo si, $y < qx/p$, o $y \leq [qx/p]$. Por lo tanto, el número de valores positivos es

$$\sum_{x=1}^{(p-1)/2} \left[\frac{qx}{p} \right].$$

Análogamente, el número de valores negativos es

$$\sum_{y=1}^{(q-1)/2} \left[\frac{py}{q} \right].$$

Puesto que el número de valores positivos y negativos es en total

$$\frac{p-1}{2} \frac{q-1}{2}$$

hemos demostrado (5) y, por ende, (4). □

Nota. El lector puede encontrar instructivo interpretar la precedente demostración de (5) geoméricamente, utilizando puntos reticulares del plano.

Por lo menos se han publicado 150 demostraciones de la ley de reciprocidad cuadrática. El propio Gauss proporcionó no menos de ocho, incluyendo una versión de la que acabamos de dar. En un artículo de M. Gerstenhaber [25] se encuentra una demostración breve de la ley de reciprocidad cuadrática.

9.6 APLICACIONES DE LA LEY DE RECIPROCIDAD

Los ejemplos que siguen muestran cómo utilizar la ley de reciprocidad cuadrática para resolver los dos tipos básicos de problemas de la teoría de restos cuadráticos.

EJEMPLO 1 Determinar si 219 es un resto cuadrático o un resto no cuadrático mod. 383.

Solución

Evaluamos el símbolo de Legendre $(219|383)$ utilizando la propiedad multiplicativa, la ley de reciprocidad, la periodicidad, y los valores especiales $(-1|p)$ y $(2|p)$ calculados anteriormente.

Como $219 = 3 \cdot 73$ la propiedad multiplicativa implica

$$(219|383) = (3|383)(73|383).$$

Utilizando la ley de reciprocidad y la periodicidad tenemos

$$(3|383) = (383|3)(-1)^{(383-1)(3-1)/4} = -(-1|3) = -(-1)^{(3-1)/2} = 1,$$

y

$$\begin{aligned}(73|383) &= (383|73)(-1)^{(383-1)(73-1)/4} = (18|73) = (2|73)(9|73) \\ &= (-1)^{((73)^2-1)/8} = 1.\end{aligned}$$

Por lo tanto $(219|383) = 1$ luego 219 es un resto cuadrático mod 383.

EJEMPLO 2. Determinar aquellos primos impares p para los que 3 es un resto cuadrático y aquellos para los que es un no resto.

Solución

De nuevo, por la ley de reciprocidad tenemos

$$(3|p) = (p|3)(-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2}(p|3).$$

Para determinar $(p|3)$ necesitamos conocer el valor de p mod 3, y para determinar $(-1)^{(p-1)/2}$ necesitamos conocer el valor de $(p-1)/2$ mod 2, o el valor de p mod 4. Por lo tanto consideramos p mod 12. Sólo debemos considerar cuatro casos, $p \equiv 1, 5, 7$ y 11 (mod 12), excluyéndose los otros casos debido a que p es impar.

Caso 1. $p \equiv 1$ (mod 12). En este caso $p \equiv 1$ (mod 3) luego $(p|3) = (1|3) = 1$. Además $p \equiv 1$ (mod 4) luego $(p-1)/2$ es par, luego $(3|p) = 1$.

Caso 2. $p \equiv 5$ (mod 12). En este caso $p \equiv 2$ (mod 3) luego $(p|3) = (2|3) = (-1)^{(3^2-1)/8} = -1$. De nuevo, $(p-1)/2$ es par ya que $p \equiv 1$ (mod 4), luego $(3|p) = -1$.

Caso 3. $p \equiv 7 \pmod{12}$. En este caso $p \equiv 1 \pmod{3}$, luego $(p|3) = (1|3) = 1$. Además $(p-1)/2$ es impar ya que $p \equiv 3 \pmod{4}$, luego $(3|p) = -1$.

Caso 4. $p \equiv 11 \pmod{12}$. En este caso $p \equiv 2 \pmod{3}$, luego $(p|3) = (2|3) = -1$. De nuevo $(p-1)/2$ es impar ya que $p \equiv 3 \pmod{4}$, luego $(3|p) = 1$.

Resumiendo estos resultados obtenemos

$$3Rp \text{ si } p \equiv \pm 1 \pmod{12}$$

$$3\bar{R}p \text{ si } p \equiv \pm 5 \pmod{12}.$$

9.7 EL SÍMBOLO DE JACOBI

Para determinar si un número compuesto es un resto cuadrático o un no resto cuadrático mod p es necesario considerar varios casos que dependen del carácter cuadrático de los factores. Es posible simplificar ciertos cálculos utilizando una extensión del símbolo de Legendre, introducida por Jacobi.

Definición. Si P es un entero positivo impar cuya descomposición en factores primos es

$$P = \prod_{i=1}^r p_i^{a_i}$$

el símbolo de Jacobi $(n|P)$ se define para todo entero n por medio de la ecuación

$$(6) \quad (n|P) = \prod_{i=1}^r (n|p_i)^{a_i},$$

en donde $(n|p_i)$ es el símbolo de Legendre. Definimos además $(n|1) = 1$.

Los posibles valores de $(n|P)$ son 1, -1 , y 0, con $(n|P) = 0$ si, y sólo si, $(n, P) > 1$. Si la congruencia

$$x^2 \equiv n \pmod{P}$$

tiene una solución, entonces $(n|p_i) = 1$ para cada primo p_i de (6), y entonces $(n|P) = 1$. Sin embargo el recíproco es falso ya que $(n|P)$ puede ser 1 si en (6) aparece un número par de factores -1 .

El lector puede comprobar que las siguientes propiedades del símbolo de Jacobi se deducen con facilidad de las propiedades del símbolo de Legendre.

Teorema 9.9 Si P y Q son enteros positivos impares, tenemos

- (a) $(m|P)(n|P) = (mn|P)$,
- (b) $(n|P)(n|Q) = (n|PQ)$,
- (c) $(m|P) = (n|P)$ si $m \equiv n \pmod{P}$,
- (d) $(a^2n|P) = (n|P)$ si $(a, P) = 1$.

Las fórmulas especiales para calcular los símbolos de Legendre $(-1|p)$ y $(2|p)$ se verifican asimismo para el símbolo de Jacobi.

Teorema 9.10 Si P es un entero positivo impar tenemos

$$(7) \quad (-1|P) = (-1)^{(P-1)/2}$$

y

$$(8) \quad (2|P) = (-1)^{(P^2-1)/8}.$$

DEMOSTRACIÓN. Escribimos $P = p_1 p_2 \dots p_m$ en donde los factores primos p_i no son necesariamente distintos. Puede escribirse también

$$P = \prod_{i=1}^m (1 + p_i - 1) = 1 + \sum_{i=1}^m (p_i - 1) + \sum_{i \neq j} (p_i - 1)(p_j - 1) + \dots$$

Pero cada factor $p_i - 1$ es par, luego cada suma salvo la primera es divisible por 4. Luego

$$P \equiv 1 + \sum_{i=1}^m (p_i - 1) \pmod{4},$$

o sea

$$\frac{1}{2}(P - 1) \equiv \sum_{i=1}^m \frac{1}{2}(p_i - 1) \pmod{2}.$$

Por consiguiente

$$(-1|P) = \prod_{i=1}^m (-1|p_i) = \prod_{i=1}^m (-1)^{(p_i-1)/2} = (-1)^{(P-1)/2},$$

que prueba (7).

Para probar (8) escribimos

$$P^2 = \prod_{i=1}^m (1 + p_i^2 - 1) = 1 + \sum_{i=1}^m (p_i^2 - 1) + \sum_{i \neq j} (p_i^2 - 1)(p_j^2 - 1) + \dots$$

Como cada p_i es impar tenemos $p_i^2 - 1 \equiv 0 \pmod{8}$ luego

$$P^2 \equiv 1 + \sum_{i=1}^m (p_i^2 - 1) \pmod{64}$$

por tanto

$$\frac{1}{8}(P^2 - 1) = \sum_{i=1}^m \frac{1}{8}(p_i^2 - 1) \pmod{8}.$$

Esto también verifica mod 2, luego

$$(2|P) = \prod_{i=1}^m (2|p_i) = \prod_{i=1}^m (-1)^{(p_i^2-1)/8} = (-1)^{(P^2-1)/8},$$

que prueba (8). □

Teorema 9.11 Ley de reciprocidad para los símbolos de Jacobi. Si P y Q son enteros positivos impares con $(P, Q) = 1$, entonces

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}.$$

DEMOSTRACIÓN. Escribimos $P = p_1 \dots p_m$, $Q = q_1 \dots q_n$, en donde los p_i y los q_i son primos. Entonces

$$(P|Q)(Q|P) = \prod_{i=1}^m \prod_{j=1}^n (p_i|q_j)(q_j|p_i) = (-1)^r,$$

Aplicando la ley de reciprocidad cuadrática a cada factor obtenemos

$$r = \sum_{i=1}^m \sum_{j=1}^n \frac{1}{2}(p_i - 1) \frac{1}{2}(q_j - 1) = \sum_{i=1}^m \frac{1}{2}(p_i - 1) \sum_{j=1}^n \frac{1}{2}(q_j - 1).$$

En la demostración del teorema 9.10 hemos demostrado que

$$\sum_{i=1}^m \frac{1}{2}(p_i - 1) \equiv \frac{1}{2}(P - 1) \pmod{2},$$

y una congruencia análoga vale para $\sum \frac{1}{2}(q_j - 1)$. Por consiguiente

$$r \equiv \frac{P-1}{2} \frac{Q-1}{2} \pmod{2},$$

que termina la demostración. $\square$

EJEMPLO 1 Determinar si 888 es un resto cuadrático o un no resto del primo 1999.

Solución

Tenemos

$$(888|1999) = (4|1999)(2|1999)(111|1999) = (111|1999).$$

Para calcular $(111|1999)$ utilizando los símbolos de Legendre escribiremos

$$(111|1999) = (3|1999)(37|1999)$$

y aplicaremos la ley de reciprocidad cuadrática a cada factor de la derecha. Con símbolos de Jacobi el cálculo es simple ya que se tiene

$$(111|1999) = -(1999|111) = -(1|111) = -1.$$

Por consiguiente 888 es un no resto cuadrático de 1999.

EJEMPLO 2. Determinar si -104 es un resto cuadrático o un no resto del primo 997.

Solución

Dado que $104 = 2 \cdot 4 \cdot 13$ tenemos

$$\begin{aligned} (-104|997) &= (-1|997)(2|997)(13|997) = -(13|997) \\ &= -(997|13) = -(9|13) = -1. \end{aligned}$$

Por consiguiente -104 es un no resto cuadrático de 997.

9.8 APLICACIONES A LAS ECUACIONES DIOFÁNTICAS

Las ecuaciones que se pueden resolver con enteros se llaman *ecuaciones diofánticas* en recuerdo de Diofanto de Alejandría. Un ejemplo lo constituye la ecuación

$$(9) \quad y^2 = x^3 + k$$

en donde k es un entero dado. El problema consiste en decidir, para un k dado, si la ecuación posee soluciones enteras x, y o si no las posee y , en caso afirmativo, determinarlas todas.

Discutiremos ahora esta ecuación, en parte porque posee una larga historia, que empieza en el siglo diecisiete, y también porque en ciertos casos se pueden tratar por medio de restos cuadráticos. Un teorema general establece que la ecuación diofántica

$$y^2 = f(x)$$

tiene a lo sumo un número finito de soluciones si $f(x)$ es un polinomio de grado ≥ 3 con coeficientes enteros y con ceros distintos. (Ver teorema 4-18 de LeVeque [44], Vol. 2.) Sin embargo no se conoce ningún método para determinar las soluciones (ni tampoco el número de soluciones) salvo en casos muy especiales. El teorema que sigue describe un conjunto infinito de valores de k para los que (9) carece de soluciones.

Teorema 9.12 *La ecuación diofántica*

$$(10) \quad y^2 = x^3 + k$$

carece de soluciones si k es de la forma

$$(11) \quad k = (4n - 1)^3 - 4m^2,$$

en donde m y n son enteros tales que ningún primo $p \equiv -1 \pmod{4}$ divide a m .

DEMOSTRACIÓN. Suponemos que existe una solución x, y y obtenemos una contradicción al considerar la ecuación módulo 4. Puesto que $k \equiv -1 \pmod{4}$ tenemos

$$(12) \quad y^2 \equiv x^3 - 1 \pmod{4}.$$

Pero $y^2 \equiv 0$ ó $1 \pmod{4}$ para cada y , luego (12) no se satisfará si x es par o si $x \equiv -1 \pmod{4}$. Por consiguiente tenemos $x \equiv 1 \pmod{4}$. Ahora sea

$$a = 4n - 1$$

con lo que $k = a^3 - 4m^2$, y escribamos (10) en la forma

$$(13) \quad y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2).$$

Puesto que $x \equiv 1 \pmod{4}$ y $a \equiv 1 \pmod{4}$ tenemos

$$(14) \quad x^2 - ax + a^2 \equiv 1 - a + a^2 \equiv -1 \pmod{4}.$$

Luego $x^2 - ax + a^2$ es impar, y (14) prueba que no es posible que todos sus factores primos sean $\equiv 1 \pmod{4}$. Por consiguiente algún factor primo $p \equiv -1 \pmod{4}$ divide a $x^2 - ax + a^2$, y (13) prueba que divide también a $y^2 + 4m^2$. Con otras palabras,

$$y^2 \equiv -4m^2 \pmod{p} \quad \text{para algún } p \equiv -1 \pmod{4}.$$

Pero $p \nmid m$ por hipótesis, por lo tanto $(-4m^2|p) = (-1|p) = -1$, en contradicción con (15). Esto demuestra que la ecuación diofántica (10) carece de soluciones cuando k tiene la forma (11). $\square$

La tabla que sigue da algunos valores de k entre los precisados por el teorema 9.12.

n	0	0	0	0	1	1	1	1	2	2	2	2
m	1	2	4	5	1	2	4	5	1	2	4	5
k	-5	-17	-65	-100	23	11	-37	-73	339	327	279	243

Nota. Se han calculado todas las soluciones de (10) cuando k se halla en el intervalo $-100 \leq k \leq 100$. (Ver referencia [32].) No existen soluciones para los valores de $k \leq 100$:

$$k = 6, 7, 11, 13, 14, 20, 21, 23, 29, 32, 34, 39, 42, 45, 46, 47, 51, 53, 58, \\ 59, 60, 61, 62, 66, 67, 69, 70, 74, 75, 77, 78, 83, 84, 85, 86, 87, 88, 90, \\ 93, 95, 96.$$

9.9 SUMAS DE GAUSS Y LEY DE RECIPROCIDAD CUADRÁTICA

En esta sección se da otra demostración de la ley de reciprocidad cuadrática con la ayuda de las sumas de Gauss

$$(16) \quad G(n, \chi) = \sum_{r \bmod p} \chi(r) e^{2\pi i n r / p},$$

en donde $\chi(r) = (r|p)$ es el carácter cuadrático mod p . Puesto que el módulo es primo, χ es un carácter primitivo y tenemos la propiedad de separabilidad

$$(17) \quad G(n, \chi) = (n|p)G(1, \chi)$$

para cada n . Además, el teorema 8.11 implica que $|G(1, \chi)|^2 = p$. El teorema que sigue demuestra que $G(1, \chi)^2$ es $\pm p$.

Teorema 9.13 Si p es un primo impar y $\chi(r) = (r|p)$ tenemos

$$(18) \quad G(1, \chi)^2 = (-1|p)p.$$

DEMOSTRACIÓN. Tenemos

$$G(1, \chi)^2 = \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} (r|p)(s|p)e^{2\pi i(r+s)/p}.$$

Para cada par r, s existe un único $t \bmod p$ tal que $s \equiv tr \pmod{p}$, y $(r|p)(s|p) = (r|p)(tr|p) = (r^2|p)(t|p) = (t|p)$. Luego

$$G(1, \chi)^2 = \sum_{t=1}^{p-1} \sum_{r=1}^{p-1} (t|p)e^{2\pi i r(1+t)/p} = \sum_{t=1}^{p-1} (t|p) \sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p}.$$

La última suma respecto de r es una suma geométrica dada por

$$\sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p} = \begin{cases} -1 & \text{si } p \nmid (1+t), \\ p-1 & \text{si } p|(1+t). \end{cases}$$

Por consiguiente

$$\begin{aligned} G(1, \chi)^2 &= - \sum_{t=1}^{p-2} (t|p) + (p-1)(p-1|p) = - \sum_{t=1}^{p-1} (t|p) + p(-1|p) \\ &= (-1|p)p \end{aligned}$$

ya que $\sum_{t=1}^{p-1} (t|p) = 0$. Esto prueba (18). $\square$

La ecuación (18) prueba que $G(1, \chi)^2$ es un entero, o sea que $G(1, \chi)^{q-1}$ también es un entero para cada q impar. El teorema que sigue prueba que ley de reciprocidad cuadrática se halla relacionada con el valor de este entero módulo q .

Teorema 9.14 Sean p y q primos impares distintos y sea χ el carácter cuadrático mod p . Entonces la ley de reciprocidad cuadrática

$$(19) \quad (q|p) = (-1)^{(p-1)(q-1)/4} (p|q)$$

es equivalente a la congruencia

$$(20) \quad G(1, \chi)^{q-1} \equiv (q|p) \pmod{q}.$$

DEMOSTRACIÓN. De (18) tenemos

$$(21) \quad G(1, \chi)^{q-1} = (-1|p)^{(q-1)/2} p^{(q-1)/2} = (-1)^{(p-1)(q-1)/4} p^{(q-1)/2}.$$

Por el criterio de Euler tenemos $p^{(q-1)/2} \equiv (p|q) \pmod{q}$ luego (21) implica

$$(22) \quad G(1, \chi)^{q-1} \equiv (-1)^{(p-1)(q-1)/4} (p|q) \pmod{q}.$$

Si (20) se verifica obtenemos

$$(q|p) \equiv (-1)^{(p-1)(q-1)/4} (p|q) \pmod{q}$$

que implica (19) ya que ambos miembros son ± 1 . Recíprocamente, si (19) se verifica entonces (22) implica (20). $\square$

El teorema que sigue da una identidad que utilizaremos para deducir (20).

Teorema 9.15 *Si p y q son primos distintos impares y χ es el carácter cuadrático mod p tenemos*

$$(23) \quad G(1, \chi)^{q-1} = (q|p) \sum_{\substack{r_1 \bmod p \\ r_1 + \dots + r_q \equiv q \pmod{p}}} \dots \sum_{r_q \bmod p} (r_1 \dots r_q | p).$$

DEMOSTRACIÓN. La suma de Gauss $G(n, \chi)$ es una función periódica de n con período p . Lo mismo ocurre a $G(n, \chi)^q$ por lo que tenemos un desarrollo finito de Fourier

$$G(n, \chi)^q = \sum_{m \bmod p} a_q(m) e^{2\pi i m n / p},$$

en donde los coeficientes vienen dados por

$$(24) \quad a_q(m) = \frac{1}{p} \sum_{n \bmod p} G(n, \chi)^q e^{-2\pi i m n / p}.$$

De la definición de $G(n, \chi)$ obtenemos

$$\begin{aligned}
 G(n, \chi)^q &= \sum_{r_1 \bmod p} (r_1 | p) e^{2\pi i n r_1 / p} \cdots \sum_{r_q \bmod p} (r_q | p) e^{2\pi i n r_q / p} \\
 &= \sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q | p) e^{2\pi i n (r_1 + \cdots + r_q) / p},
 \end{aligned}$$

por lo que (24) se transforma en

$$a_q(m) = \frac{1}{p} \sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q | p) \sum_{n \bmod p} e^{2\pi i n (r_1 + \cdots + r_q - m) / p}.$$

La suma respecto de n es una suma geométrica que únicamente se anula cuando $r_1 + \cdots + r_q \equiv m \pmod{p}$, en cuyo caso la suma es igual a p . Luego

$$(25) \quad a_q(m) = \sum_{\substack{r_1 \bmod p \\ r_1 + \cdots + r_q \equiv m \pmod{p}}} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q | p).$$

Ahora volvemos a (24) y obtenemos otra expresión para $a_q(m)$. Utilizando la separabilidad de $G(n, \chi)$ y la relación $(n|p)^q = (n|p)$ para q impar obtenemos

$$\begin{aligned}
 a_q(m) &= \frac{1}{p} G(1, \chi)^q \sum_{n \bmod p} (n|p) e^{-2\pi i m n / p} = \frac{1}{p} G(1, \chi)^q G(-m, \chi) \\
 &= \frac{1}{p} G(1, \chi)^q (m|p) G(-1, \chi) = (m|p) G(1, \chi)^{q-1}.
 \end{aligned}$$

ya que

$$G(1, \chi) G(-1, \chi) = G(1, \chi) \overline{G(1, \chi)} = |G(1, \chi)|^2 = p.$$

Con otras palabras, $G(1, \chi)^{q-1} = (m|p) a_q(m)$. Si hacemos $m = q$ y utilizamos (25) obtenemos (23). $\square$

Demostración de la ley de reciprocidad. Para deducir la ley de reciprocidad cuadrática a partir de (23) es suficiente demostrar que

$$(26) \quad \sum_{r_1 \bmod p} \cdots \sum_{r_q \bmod p} (r_1 \cdots r_q | p) \equiv 1 \pmod{q},$$

en donde los índices de sumación $r_1, \dots, r_q$ se hallan sujetos a la restricción

$$(27) \quad r_1 + \cdots + r_q \equiv q \pmod{p}.$$

Si todos los índices $r_1, \dots, r_q$ son congruentes unos con otros mod p , entonces su suma es congruente a qr_j para cada $j = 1, 2, \dots, q$, luego (27) se verifica si, y sólo si,

$$qr_j \equiv q \pmod{p},$$

esto es, si, y sólo si, $r_j \equiv 1 \pmod{p}$ para cada j . En este caso el sumando correspondiente de (26) es $(1|p) = 1$. Para cualquier otra elección de índices que satisfaga (27) debe haber por lo menos dos índices incongruentes entre los $r_1, \dots, r_q$. Por consiguiente cada permutación cíclica de $r_1, \dots, r_q$ origina una nueva solución de (27) que proporciona el mismo sumando, $(r_1 \cdots r_q|p)$. Por lo que cada sumando aparece q veces y aporta mod q el valor 0 a la suma. Luego la única aportación en la suma de (26) que no es cero módulo q es $(1|p) = 1$. Esto completa la demostración. $\square$

9.10 LEY DE RECIPROCIDAD PARA SUMAS CUADRÁTICAS DE GAUSS

Esta sección describe otra demostración de la ley de reciprocidad cuadrática basada en las sumas cuadráticas de Gauss

$$(28) \quad G(n; m) = \sum_{r=1}^m e^{2\pi i n r^2 / m}.$$

Si p es un número primo impar y $p \nmid n$ tenemos la fórmula

$$(29) \quad G(n; p) = (n|p)G(1; p)$$

que reduce el estudio de las sumas $G(n; p)$ al caso $n = 1$. La ecuación (29) se sigue fácilmente de (28) teniendo presente que $G(n; p) = G(n, \chi)$, en donde $\chi(n) = (n|p)$, y observando que $G(n, \chi)$ es separable.

Aunque cada término de la suma $G(1; p)$ tiene valor absoluto 1, la suma en sí tiene valor absoluto 0, $\sqrt{p}$ o $\sqrt{2p}$. De hecho, Gauss demostró para cada $m \geq 1$ la siguiente fórmula importante

$$(30) \quad G(1; m) = \frac{1}{2} \sqrt{m} (1 + i) (1 + e^{-\pi i m / 2}) = \begin{cases} \sqrt{m} & \text{si } m \equiv 1 \pmod{4} \\ 0 & \text{si } m \equiv 2 \pmod{4} \\ i\sqrt{m} & \text{si } m \equiv 3 \pmod{4} \\ (1 + i)\sqrt{m} & \text{si } m \equiv 0 \pmod{4} \end{cases}$$

Se conocen varias demostraciones distintas de (30). Deduiremos (30) analizando una suma relacionada con la cuestión

$$S(a, m) = \sum_{r=0}^{m-1} e^{\pi i a r^2 / m},$$

en donde a y m son enteros positivos. Si $a = 2$, entonces $S(2, m) = G(1; m)$.

Las sumas $S(a, m)$ disfrutan de una ley de reciprocidad (establecida a continuación del teorema 9.16) que implica la fórmula de Gauss (30) y además proporciona otra demostración de la ley de reciprocidad cuadrática.

Teorema 9.16 *Si el producto ma es par, tenemos*

$$(31) \quad S(a, m) = \sqrt{\frac{m}{a}} \left(\frac{1+i}{\sqrt{2}} \right) \overline{S(m, a)},$$

en donde la barra designa el complejo conjugado.

Nota. Para deducir la fórmula de Gauss (30) tomamos $a = 2$ en (31) y observamos que $\overline{S(m, 2)} = 1 + e^{-\pi i m/2}$.

DEMOSTRACIÓN. Esta demostración se basa en el cálculo de residuos. Sea g la función definida por la ecuación

$$(32) \quad g(z) = \sum_{r=0}^{m-1} e^{\pi i a (z+r)^2 / m}.$$

Entonces g es analítica para todo valor de z , y $g(0) = S(a, m)$. Puesto que ma es par obtenemos

$$g(z+1) - g(z) = e^{\pi i a z^2 / m} (e^{2\pi i a z} - 1) = e^{\pi i a z^2 / m} (e^{2\pi i z} - 1) \sum_{n=0}^{a-1} e^{2\pi i n z}.$$

Ahora definimos f por medio de la ecuación

$$f(z) = \frac{g(z)}{e^{2\pi i z} - 1}.$$

Entonces f es analítica para todo z excepto en un polo de primer orden en cada entero, y f satisface la ecuación

$$(33) \quad f(z+1) = f(z) + \varphi(z),$$

en donde

$$(34) \quad \varphi(z) = e^{\pi i a z^2 / m} \sum_{n=0}^{a-1} e^{2\pi i n z}.$$

La función φ es analítica para todo z .

En $z = 0$ el residuo de f es $g(0)/(2\pi i)$ y por lo tanto

$$(35) \quad S(a, m) = g(0) = 2\pi i \operatorname{Res}_{z=0} f(z) = \int_{\gamma} f(z) dz,$$

en donde γ es un arco simple cerrado y orientado positivamente cuyo grafo únicamente contiene el polo $z = 0$ en su región interior. Elegiremos γ de forma que describa un paralelogramo de vértices $A, A + 1, B + 1, B$ en donde

$$A = -\frac{1}{2} - Re^{\pi i/4} \quad \text{y} \quad B = -\frac{1}{2} + Re^{\pi i/4},$$

tal como se dibuja en la figura 9.1. Integrando f a lo largo de γ obtenemos

$$\int_{\gamma} f = \int_A^{A+1} f + \int_{A+1}^{B+1} f + \int_{B+1}^B f + \int_B^A f.$$

En la integral $\int_{A+1}^{B+1} f$ efectuamos el cambio de variable $w = z + 1$ y utilizando (33) obtenemos

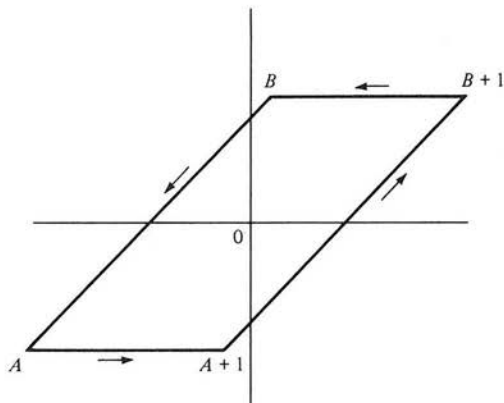


Figura 9.1

$$\int_{A+1}^{B+1} f(w) dw = \int_A^B f(z+1) dz = \int_A^B f(z) dz + \int_A^B \varphi(z) dz.$$

Por consiguiente (35) proporciona

$$(36) \quad S(a, m) = \int_A^B \varphi(z) dz + \int_A^{A+1} f(z) dz - \int_B^{B+1} f(z) dz.$$

Ahora probaremos que las integrales a lo largo de los segmentos horizontales que unen A con $A+1$ y B con $B+1$ tienden a 0 cuando $R \rightarrow +\infty$. Para ello acotamos el integrando sobre tales segmentos. Escribimos

$$(37) \quad |f(z)| = \frac{|g(z)|}{|e^{2\pi iz} - 1|},$$

y acotamos separadamente el numerador y el denominador.

Sobre el segmento que une B con $B+1$ obtenemos

$$\gamma(t) = t + Re^{\pi i/4}, \text{ en donde } -\frac{1}{2} \leq t \leq \frac{1}{2}.$$

De (32) obtenemos

$$(38) \quad |g[\gamma(t)]| \leq \sum_{r=0}^{m-1} \left| \exp \left\{ \frac{\pi i a(t + Re^{\pi i/4} + r)^2}{m} \right\} \right|,$$

en donde $\exp z = e^z$. La expresión entre paréntesis tiene como parte real

$$\frac{-\pi a(\sqrt{2}tR + R^2 + \sqrt{2}rR)}{m}.$$

Dado que $|e^{x+iy}| = e^x$ y $\exp \{-\pi a \sqrt{2} rR/m\} \leq 1$, cada término de (38) tiene valor absoluto que no excede a $\exp \{-\pi a R^2/m\} \exp \{-\sqrt{2} \pi a tR/m\}$. Pero $-\frac{1}{2} \leq t \leq \frac{1}{2}$, por lo que obtenemos la acotación

$$|g[\gamma(t)]| \leq m e^{\pi \sqrt{2} a R/(2m)} e^{-\pi a R^2/m}.$$

Para el denominador de (37) utilizamos la desigualdad triangular en la forma

$$|e^{2\pi iz} - 1| \geq ||e^{2\pi iz}| - 1|.$$

Dado que $|\exp \{2\pi i \gamma(t)\}| = \exp \{-2\pi R \sin(\pi/4)\} = \exp \{-\sqrt{2}\pi R\}$, obtenemos

$$|e^{2\pi i \gamma(t)} - 1| \geq 1 - e^{-\sqrt{2}\pi R}.$$

Por consiguiente sobre el segmento que une B con $B + 1$ tenemos la acotación

$$|f(z)| \leq \frac{me^{\pi\sqrt{2}aR/(2m)}e^{-\pi aR^2/m}}{1 - e^{-\sqrt{2}\pi R}} = o(1) \quad \text{cuando } R \rightarrow +\infty.$$

Un razonamiento análogo prueba que el integrando tiende a 0 sobre el segmento que une A con $A + 1$ cuando $R \rightarrow +\infty$. Como la longitud del arco de integración es 1 en cada caso, resulta que la segunda y tercera integral de la derecha de (36) tienden a 0 cuando $R \rightarrow +\infty$. Por consiguiente podemos escribir (36) en la forma

$$(39) \quad S(a, m) = \int_A^B \varphi(z) dz + o(1) \quad \text{cuando } R \rightarrow +\infty.$$

Para tratar la integral $\int_A^B \varphi$ aplicamos el teorema de Cauchy, integrando φ a lo largo del paralelogramo de vértices $A, B, \alpha, -\alpha$, en donde $\alpha = B + \frac{1}{2} = Re^{\pi i/4}$. (Ver figura 9.2.) Puesto que ϵ es analítica para todo z , su integral a lo largo de este paralelogramo es 0, o sea

$$(40) \quad \int_A^B \varphi + \int_B^\alpha \varphi + \int_\alpha^{-\alpha} \varphi + \int_{-\alpha}^A \varphi = 0.$$

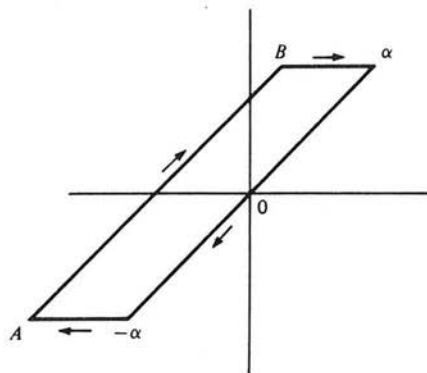


Figura 9.2

Debido al factor exponencial $e^{\pi iz^2/m}$ de (34), un razonamiento análogo al dado anteriormente prueba que la integral de φ a lo largo de cada segmento horizontal $\rightarrow 0$ cuando $R \rightarrow +\infty$. Por consiguiente (40) nos proporciona

$$\int_A^B \varphi = \int_{-\alpha}^{\alpha} \varphi + o(1) \quad \text{cuando } R \rightarrow +\infty,$$

y (39) se transforma en

$$(41) \quad S(a, m) = \int_{-\alpha}^{\alpha} \varphi(z) dz + o(1) \quad \text{cuando } R \rightarrow +\infty,$$

en donde $\alpha = Re^{\pi i/4}$. Usando (34) obtenemos

$$\int_{-\alpha}^{\alpha} \varphi(z) dz = \sum_{n=0}^{a-1} \int_{-\alpha}^{\alpha} e^{\pi i az^2/m} e^{2\pi i n z} dz = \sum_{n=0}^{a-1} e^{-\pi i mn^2/a} I(a, m, n, R),$$

en donde

$$I(a, m, n, R) = \int_{-\alpha}^{\alpha} \exp\left\{\frac{\pi i a}{m} \left(z + \frac{nm}{a}\right)^2\right\} dz.$$

Aplicando de nuevo el teorema de Cauchy al paralelogramo de vértices $-\alpha$, α , $\alpha - (nm/a)$, y $-\alpha - (nm/a)$, vemos como antes que las integrales a lo largo de los segmentos horizontales $\rightarrow 0$ cuando $R \rightarrow +\infty$, por lo que

$$I(a, m, n, R) = \int_{-\alpha - nm/a}^{\alpha - nm/a} \exp\left\{\frac{\pi i a}{m} \left(z + \frac{nm}{a}\right)^2\right\} dz + o(1) \quad \text{cuando } R \rightarrow +\infty.$$

El cambio de variable $w = \sqrt{a/m}(z + (nm/a))$ transforma esto en la forma

$$I(a, m, n, R) = \sqrt{\frac{m}{a}} \int_{-\alpha\sqrt{a/m}}^{\alpha\sqrt{a/m}} e^{\pi i w^2} dw + o(1) \quad \text{cuando } R \rightarrow +\infty.$$

Si en (41) hacemos que $R \rightarrow +\infty$, obtenemos

$$(42) \quad S(a, m) = \sum_{n=0}^{a-1} e^{-\pi i mn^2/a} \sqrt{\frac{m}{a}} \lim_{R \rightarrow +\infty} \int_{-R\sqrt{a/m}e^{\pi i/4}}^{R\sqrt{a/m}e^{\pi i/4}} e^{\pi i w^2} dw.$$

Escribiendo $T = \sqrt{a/m}R$, vemos que el último límite es igual a

$$\lim_{T \rightarrow +\infty} \int_{-Te^{\pi i/4}}^{Te^{\pi i/4}} e^{\pi i w^2} dw = I$$

en donde I es un número que no depende ni de a ni de m . Por consiguiente (42) nos da

$$(43) \quad S(a, m) = \sqrt{\frac{m}{a}} \overline{IS(m, a)}.$$

Para evaluar I hacemos $a = 1$ y $m = 2$ en (43). Entonces $S(1, 2) = 1 + i$ y $S(2, 1) = 1$, luego (43) implica $I = (1 + i)/\sqrt{2}$, y (43) se reduce a (31). $\square$

El teorema 9.16 implica una ley de reciprocidad para sumas cuadráticas de Gauss.

Teorema 9.17. Si $h > 0$, $k > 0$, h impar. entonces

$$(44) \quad G(h; k) = \sqrt{\frac{k}{h}} \frac{1+i}{2} (1 + e^{-\pi i h k / 2}) \overline{G(k; h)}.$$

DEMOSTRACIÓN. Tomamos $a = 2h$, $m = k$ en el teorema 9.16 para obtener

$$(45) \quad G(h; k) = S(2h, k) = \sqrt{\frac{k}{2h}} \frac{1+i}{\sqrt{2}} \overline{S(k, 2h)} = \sqrt{\frac{k}{h}} \frac{1+i}{2} \sum_{r=0}^{2h-1} e^{-\pi i k r^2 / (2h)}.$$

Descomponemos la suma respecto de r en dos partes correspondientes a los r pares e impares. Para r par escribimos $r = 2s$, en donde $s = 0, 1, \dots, h-1$. Para r impar observamos que $(r + 2h)^2 \equiv r^2 \pmod{4h}$ por lo que la suma se puede extender a los números impares de cualquier sistema residual completo mod $2h$. Sumamos respecto de tales números impares en el intervalo $h \leq r < 3h$, haciendo $r = 2s + h$, en donde $s = 0, 1, 2, \dots, h-1$. (Los números $2s + h$ son impares y distintos mod $2h$.) Esto nos da

$$\begin{aligned} \sum_{r=0}^{2h-1} e^{-\pi i k r^2 / (2h)} &= \sum_{s=0}^{h-1} e^{-\pi i k (2s)^2 / (2h)} + \sum_{s=0}^{h-1} e^{-\pi i k (2s+h)^2 / (2h)} \\ &= \sum_{s=0}^{h-1} e^{-2\pi i k s^2 / h} (1 + e^{-\pi i h k / 2}) \\ &= (1 + e^{-\pi i h k / 2}) \overline{G(k; h)}. \end{aligned}$$

Utilizando este resultado en (45) obtenemos (44). $\square$

9.11 OTRA DEMOSTRACIÓN DE LA LEY DE RECIPROCIDAD CUADRÁTICA

La fórmula de Gauss (30) nos proporciona una demostración rápida de la ley de reciprocidad cuadrática. En primer lugar observamos que (30) implica

$$G(1; k) = i^{(k-1)^2/4} \sqrt{k}$$

si k es impar. Además, tenemos la propiedad multiplicativa (ver ejercicio 8.16(a))

$$G(m; n)G(n; m) = G(1; mn) \quad \text{si } (m, n) = 1.$$

Por consiguiente, si p y q son primos impares distintos tenemos

$$G(p; q) = (p|q)G(1; q) = (p|q)i^{(q-1)^2/4} \sqrt{q}$$

$$G(q; p) = (q|p)G(1; p) = (q|p)i^{(p-1)^2/4} \sqrt{p}$$

y

$$G(p; q)G(q; p) = G(1; pq) = i^{(pq-1)^2/4} \sqrt{pq}.$$

Comparando esta última ecuación con las dos anteriores obtenemos

$$(p|q)(q|p)i^{((q-1)^2 + (p-1)^2)/4} = i^{(pq-1)^2/4},$$

y la ley de reciprocidad cuadrática se sigue observando que

$$i^{((pq-1)^2 - (q-1)^2 - (p-1)^2)/4} = (-1)^{(p-1)(q-1)/4}.$$

□

Ejercicios del capítulo 9

1. Determinar los primos impares p para los que $(-3|p) = 1$ y aquellos para los que $(-3|p) = -1$.
2. Probar que 5 es un resto cuadrático de un primo impar p si $p \equiv \pm 1 \pmod{10}$, y que 5 es un no resto cuadrático si $p \equiv \pm 3 \pmod{10}$.
3. Sea p un primo impar. Suponemos que el conjunto $\{1, 2, \dots, p-1\}$ se puede expresar como reunión de dos subconjuntos S y T , $S \neq T$, tales que el producto $(\text{mod } p)$ de cada dos elementos del mismo conjunto pertenece a S , mientras que el producto $(\text{mod } p)$ de un elemento de S por un elemento de T pertenece a T . Probar que S consta de los restos cuadráticos y T de los no restos cuadráticos $\text{mod } p$.
4. Sea $f(x)$ un polinomio que toma valores enteros cuando x es entero.
 - (a) Si a y b son enteros, probar que

$$\sum_{x \bmod p} (f(ax+b)|p) = \sum_{x \bmod p} (f(x)|p) \quad \text{si } (a, p) = 1,$$

y que

$$\sum_{x \bmod p} (af(x)|p) = (a|p) \sum_{x \bmod p} (f(x)|p) \quad \text{para todo } a.$$

(b) Probar que

$$\sum_{x \bmod p} (ax+b|p) = 0 \quad \text{si } (a, p) = 1.$$

(c) Sea $f(x) = x(ax+b)$, en donde $(a, p) = (b, p) = 1$. Probar que

$$\sum_{x=1}^{p-1} (f(x)|p) = \sum_{x=1}^{p-1} (a+bx|p) = -(a|p).$$

[Indicación: Cuando x barre un sistema residual reducido mod p , también lo barre x' , inverso de $x \bmod p$.]

5. Sean α y β enteros cuyos valores posibles son ± 1 . Sea $N(\alpha, \beta)$ el número de enteros x de $\{1, 2, \dots, p-2\}$ tales que

$$(x|p) = \alpha \quad \text{y} \quad (x+1|p) = \beta,$$

en donde p es un primo impar. Probar que

$$4N(\alpha, \beta) = \sum_{x=1}^{p-2} \{1 + \alpha(x|p)\} \{1 + \beta(x+1|p)\},$$

y usar el ejercicio 4 para deducir que

$$4N(\alpha, \beta) = p - 2 - \beta - \alpha\beta - \alpha(-1|p).$$

En particular esto nos da

$$N(1, 1) = \frac{p-4-(-1|p)}{4},$$

$$N(-1, -1) = N(-1, 1) = \frac{p-2+(-1|p)}{4},$$

$$N(1, -1) = 1 + N(1, 1).$$

6. Utilizar el ejercicio 5 para probar que para cada primo p existen enteros x e y tales que $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.
7. Sea p un primo impar. Probar cada una de las afirmaciones siguientes:

$$(a) \sum_{r=1}^{p-1} r(r|p) = 0 \quad \text{si } p \equiv 1 \pmod{4}.$$

$$(b) \sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4} \quad \text{si } p \equiv 1 \pmod{4}.$$

$$(c) \sum_{r=1}^{p-1} r^2(r|p) = p \sum_{r=1}^{p-1} r(r|p) \quad \text{si } p \equiv 3 \pmod{4}.$$

$$(d) \sum_{r=1}^{p-1} r^3(r|p) = \frac{3}{2} p \sum_{r=1}^{p-1} r^2(r|p) \quad \text{si } p \equiv 1 \pmod{4}.$$

$$(e) \sum_{r=1}^{p-1} r^4(r|p) = 2p \sum_{r=1}^{p-1} r^3(r|p) - p^2 \sum_{r=1}^{p-1} r^2(r|p) \quad \text{si } p \equiv 3 \pmod{4}.$$

[Indicación: $p-r$ recorre los números $1, 2, \dots, p-1$ con r .]

8. Sea p un primo impar, $p \equiv 3 \pmod{4}$, y sea $q = (p-1)/2$.

(a) Probar que

$$\{1 - 2(2|p)\} \sum_{r=1}^q r(r|p) = p \frac{1 - (2|p)}{2} \sum_{r=1}^q (r|p).$$

[Indicación: Cuando r recorre los números $1, 2, \dots, q$ entonces r y $p-r$ recorren conjuntamente los números $1, 2, \dots, p-1$, así como $2r$ y $p-2r$.]

(b) Probar que

$$\{(2|p) - 2\} \sum_{r=1}^{p-1} r(r|p) = p \sum_{r=1}^q (r|p).$$

9. Si p es un primo impar, sea $\chi(n) = (n|p)$. Probar que la suma de Gauss $G(n, \chi)$ asociada a χ es la misma que la suma cuadrática de Gauss $G(n; p)$ introducida en el ejercicio 8.16 si $(n, p) = 1$. Con otras palabras, si $p \nmid n$ tenemos

$$G(n, \chi) = \sum_{m \bmod p} \chi(m) e^{2\pi i m n / p} = \sum_{r=1}^p e^{2\pi i n r^2 / p} = G(n; p).$$

Obsérvese que $G(n, \chi) \neq G(n; p)$ si $p|n$ ya que $G(p, \chi) = 0$ pero $G(p; p) = p$.

10. Calcular la suma cuadrática de Gauss $G(2; p)$ utilizando una de las leyes de reciprocidad. Comparar este resultado con la fórmula $G(2; p) = (2|p)G(1; p)$ y deducir que $(2|p) = (-1)^{(p^2-1)/8}$ si p es un primo impar.

Capítulo 10

Raíces primitivas

10.1 EL EXPONENTE DE UN NÚMERO $\bmod m$. RAÍCES PRIMITIVAS

Sean a y m enteros primos entre sí, con $m \geq 1$, y consideremos todas las potencias positivas de a :

$$a, a^2, a^3, \dots$$

Por el teorema de Euler-Fermat sabemos que $a^{\varphi(m)} \equiv 1 \pmod{m}$. Por lo menos debe existir una potencia suficientemente avanzada a^f tal que $a^f \equiv 1 \pmod{m}$. Nos interesa el menor positivo f con esta propiedad.

Definición. El menor entero positivo f tal que

$$a^f \equiv 1 \pmod{m}$$

se llama exponente de a módulo m , y se designa por

$$f = \exp_m(a).$$

Si $\exp_m(a) = \varphi(m)$, entonces a se llama raíz primitiva $\bmod m$.

El teorema de Euler-Fermat nos dice que $\exp_m(a) \leq \varphi(m)$. El teorema que sigue demuestra que $\exp_m(a)$ divide a $\varphi(m)$.

Teorema 10.1 Dado $m \geq 1$, $(a, m) = 1$, sea $f = \exp_m(a)$. Entonces tenemos:

- (a) $a^k \equiv a^h \pmod{m}$ si, y sólo si, $k \equiv h \pmod{f}$.
- (b) $a^k \equiv 1 \pmod{m}$ si, y sólo si, $k \equiv 0 \pmod{f}$. En particular, $f | \varphi(m)$.
- (c) Los números $1, a, a^2, \dots, a^{f-1}$ son incongruentes mod m .

DEMOSTRACIÓN. Las partes (b) y (c) se siguen inmediatamente de (a). Por tanto sólo necesitamos probar (a). Si $a^k \equiv a^h \pmod{m}$, entonces $a^{k-h} \equiv 1 \pmod{m}$. Escribimos

$$k - h = qf + r, \text{ en donde } 0 \leq r < f.$$

Entonces $1 \equiv a^{k-h} = a^{qf+r} \equiv a^r \pmod{m}$, luego $r = 0$ y $k \equiv h \pmod{f}$.

Recíprocamente, si $k \equiv h \pmod{f}$, entonces $k - h = qf$, luego $a^{k-h} \equiv 1 \pmod{m}$ y por lo tanto $a^k \equiv a^h \pmod{m}$. $\square$

10.2 RAÍCES PRIMITIVAS Y SISTEMAS RESIDUALES REDUCIDOS

Teorema 10.2 Sea $(a, m) = 1$. Entonces a es una raíz primitiva mod m si, y sólo si, los números

$$(1) \quad a, a^2, \dots, a^{\varphi(m)}$$

forman un sistema residual reducido mod m .

DEMOSTRACIÓN. Si a es una raíz primitiva, los números de (1) son incongruentes mod m , por el teorema 10.1(c). Como quiera que hay $\varphi(m)$ de tales números, constituyen un sistema residual reducido mod m .

Recíprocamente, si los números de (1) forman un sistema residual reducido, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$ pero ninguna potencia inferior es congruente con 1, luego a es una raíz primitiva. $\square$

Nota. En el capítulo 6 vimos que las clases residuales mod m forman un grupo. Si m admite una raíz primitiva a , el teorema 10.2 prueba que este grupo es un grupo cíclico generado por la clase residual $\bar{a}$.

La importancia de las raíces primitivas queda puesta de manifiesto por el teorema 10.2. Si m admite una raíz primitiva entonces cada sistema residual reducido mod m se puede expresar en forma de progresión geométrica. Esto proporciona una herramienta potente que puede ser manejada en aquellos problemas que con-

tienen sistemas residuales reducidos. Por desgracia, no todos los módulos poseen raíces primitivas. En las secciones que siguen probaremos que sólo admiten raíces primitivas los módulos de la forma

$$m = 1, 2, 4, p^{\alpha}, \text{ y } 2p^{\alpha},$$

en donde p es un primo impar y $\alpha \geq 1$.

Los tres primeros casos se establecen con facilidad. El caso $m = 1$ es trivial. Para $m = 2$ el número 1 es una raíz primitiva. Para $m = 4$ tenemos $\varphi(4) = 2$ y $3^2 \equiv 1 \pmod{4}$, luego 3 es una raíz primitiva. Ahora veremos que, si $\alpha \geq 3$, no existen raíces primitivas mod 2^{α} .

10.3 LA NO EXISTENCIA DE RAÍCES PRIMITIVAS mod 2^{α} PARA $\alpha \geq 3$

Teorema 10.3 *Sea x un entero impar. Si $\alpha \geq 3$ tenemos*

$$(2) \quad x^{\varphi(2^{\alpha})/2} \equiv 1 \pmod{2^{\alpha}},$$

luego no existen raíces primitivas mod 2^{α} .

DEMOSTRACIÓN. Si $\alpha = 3$, la congruencia (2) establece que $x^2 \equiv 1 \pmod{8}$ para x impar. Este hecho se comprueba fácilmente haciendo $x = 1, 3, 5, 7$ u observando que

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$$

y teniendo en cuenta que $k(k + 1)$ es par.

Ahora demostraremos el teorema por inducción sobre α . Suponemos que (2) se verifica para α y demostramos que también se verifica para $\alpha + 1$. La hipótesis de inducción nos dice que

$$x^{\varphi(2^{\alpha})/2} = 1 + 2^{\alpha}t,$$

en donde t es un entero. Elevando ambos miembros al cuadrado obtenemos

$$x^{\varphi(2^{\alpha+1})} = 1 + 2^{\alpha+1}t + 2^{2\alpha}t^2 \equiv 1 \pmod{2^{\alpha+1}}$$

ya que $2\alpha \geq \alpha + 1$. Esto termina la demostración puesto que $\varphi(2^{\alpha}) = 2^{\alpha-1} = \varphi(2^{\alpha+1})/2$. □

10.4 LA EXISTENCIA DE RAÍCES PRIMITIVAS mod p PARA PRIMOS IMPARES p

Ante todo demostraremos el siguiente lema.

Lema 1 *Dados a y m con $(a, m) = 1$, sea $f = \exp_m(a)$. Entonces*

$$\exp_m(a^k) = \frac{\exp_m(a)}{(k, f)}.$$

En particular, $\exp_m(a^k) = \exp_m(a)$ si, y sólo si, $(k, f) = 1$.

DEMOSTRACIÓN. El exponente de a^k es el menor entero positivo x tal que

$$a^{kx} \equiv 1 \pmod{m}.$$

Es también el menor $x > 0$ tal que $kx \equiv 0 \pmod{f}$. Pero esta última congruencia es equivalente a la congruencia

$$x \equiv 0 \pmod{\frac{f}{d}},$$

en donde $d = (k, f)$. La menor solución positiva de esta congruencia es f/d , luego $\exp_m(a^k) = f/d$, tal como habíamos afirmado. $\square$

El lema 1 se utilizará para demostrar la existencia de raíces primitivas para módulos primos. De hecho determinaremos el número exacto de raíces primitivas mod p .

Teorema 10.4 *Sea p un primo impar y sea d un divisor positivo de $p - 1$. Entonces en cada sistema residual reducido mod p tenemos exactamente $\varphi(d)$ números tales que*

$$\exp_p(a) = d.$$

En particular, cuando $d = \varphi(p) = p - 1$ tenemos exactamente $\varphi(p - 1)$ raíces primitivas.

DEMOSTRACIÓN. Usamos el método empleado en el capítulo 2 para probar la relación

$$\sum_{d|n} \varphi(d) = n.$$

Los números $1, 2, \dots, p-1$ se hallan distribuidos en conjuntos disjuntos $A(d)$, correspondiendo cada uno de ellos a un divisor d de $p-1$. Aquí definimos

$$A(d) = \{x : 1 \leq x \leq p-1 \text{ y } \exp_p(x) = d\}.$$

Sea $f(d)$ el número de elementos de $A(d)$. Entonces $f(d) \geq 0$ para cada d . Nuestro propósito consiste en demostrar que $f(d) = \varphi(d)$.

Como los conjuntos $A(d)$ son disjuntos y cada $x = 1, 2, \dots, p-1$ pertenece a algún $A(d)$, tenemos

$$\sum_{d|p-1} f(d) = p-1.$$

Pero también tenemos

$$\sum_{d|p-1} \varphi(d) = p-1$$

luego

$$\sum_{d|p-1} \{\varphi(d) - f(d)\} = 0.$$

Para demostrar que cada término de esta suma es cero es suficiente demostrar que $f(d) \leq \varphi(d)$. Para ello basta ver que $f(d) = 0$ o $f(d) = \varphi(d)$; o, con otras palabras, que $f(d) \neq 0$ implica $f(d) = \varphi(d)$.

Suponemos que $f(d) \neq 0$. Entonces $A(d)$ es no vacío, luego, para algún a , $a \in A(d)$. Por consiguiente

$$\exp_p(a) = d, \quad \text{por lo tanto } a^d \equiv 1 \pmod{p}.$$

Pero cada potencia de a satisface la misma congruencia, luego los d números

$$(3) \quad a, a^2, \dots, a^d$$

son soluciones de la congruencia polinómica

$$(4) \quad x^d - 1 \equiv 0 \pmod{p},$$

y estas soluciones son incongruentes mod p ya que $d = \exp_p(a)$. Pero (4) a lo sumo tiene d soluciones pues el módulo es primo, por lo que los d números de (3) deben ser *todas* las soluciones de (4). Luego cada número de $A(d)$ deberá ser de la forma a^k para un $k = 1, 2, \dots, d$. ¿Cuándo $\exp_p(a^k) = d$? De acuerdo con el lema 1 ocurrirá si, y sólo si, $(k, d) = 1$. Con otras palabras, entre los d números de (3) hay $\varphi(d)$ que tienen exponente d mod p . Luego hemos demostrado que $f(d) = \varphi(d)$ si $f(d) \neq 0$. Como hemos indicado anteriormente, esto termina la demostración. $\square$

10.5 RAÍCES PRIMITIVAS Y RESTOS CUADRÁTICOS

Teorema 10.5 *Sea g una raíz primitiva mod p , en donde p es un primo impar. Entonces las potencias pares*

$$g^2, g^4, \dots, g^{p-1}$$

son los restos cuadráticos mod p , y las potencias impares

$$g, g^3, \dots, g^{p-2}$$

son los no restos cuadráticos mod p .

DEMOSTRACIÓN. Si n es par, $n = 2m$, entonces $g^n = (g^m)^2$ luego

$$g^n \equiv x^2 \pmod{p}, \text{ en donde } x = g^m.$$

Luego $g^n R p$. Pero hay $(p-1)/2$ potencias pares distintas $g^2, \dots, g^{p-1}$ módulo p y el mismo número de restos cuadráticos mod p . Por consiguiente las potencias pares son los restos cuadráticos y las potencias impares los no restos cuadráticos. $\square$

10.6 LA EXISTENCIA DE RAÍCES PRIMITIVAS mod p^α

Ahora volvemos al caso $m = p^\alpha$, en donde p es un primo impar y $\alpha \geq 2$. Al buscar raíces primitivas mod p^α es natural considerar como posibles las raíces primitivas mod p . Si g es una de estas raíces, nos preguntamos cuando g será también una raíz primitiva mod p^2 . Ahora bien $g^{p-1} \equiv 1 \pmod{p}$ y, dado que $\varphi(p^2) = p(p-1) > p-1$, tenemos que dicha g no es ciertamente una raíz primitiva mod p^2 si $g^{p-1} \equiv 1 \pmod{p^2}$. Por consiguiente la relación

$$g^{p-1} \not\equiv 1 \pmod{p^2}$$

es una condición *necesaria* para que una raíz primitiva mod p sea también una raíz primitiva mod p^2 . Es importante observar que esta condición también es *suficiente* para que g sea una raíz primitiva mod p^2 y, en general, mod p^α para todas las potencias $\alpha \geq 2$. En efecto, tenemos el siguiente teorema.

Teorema 10.6 *Sea p un primo impar. Entonces tenemos:*

(a) *Si g es una raíz primitiva mod p , entonces g es también una raíz primitiva mod p^α para todo $\alpha \geq 1$ si, y sólo si,*

$$(5) \quad g^{p-1} \not\equiv 1 \pmod{p^2}.$$

(b) *Por lo menos existe una raíz primitiva g mod p que satisface (5), luego por lo menos existe una raíz primitiva mod p^α si $\alpha \geq 2$.*

DEMOSTRACIÓN. Primero demostraremos (b). Sea g una raíz primitiva mod p . Si $g^{p-1} \not\equiv 1 \pmod{p^2}$ no hay nada que probar. Ahora bien, si $g^{p-1} \equiv 1 \pmod{p^2}$, observamos que $g_1 = g + p$, que es otra raíz primitiva módulo p , satisface la condición

$$g_1^{p-1} \not\equiv 1 \pmod{p^2}.$$

En efecto, tenemos

$$\begin{aligned} g_1^{p-1} &= (g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + tp^2 \\ &\equiv g^{p-1} + (p^2 - p)g^{p-2} \pmod{p^2} \\ &\equiv 1 - pg^{p-2} \pmod{p^2}. \end{aligned}$$

Pero no es posible $pg^{p-2} \equiv 0 \pmod{p^2}$ ya que ello implicaría $g^{p-2} \equiv 0 \pmod{p}$, en contradicción con el hecho de que g es una raíz primitiva mod p . Luego $g^{p-1} \not\equiv 1 \pmod{p^2}$, con lo que (b) queda demostrado.

Ahora veamos (a). Sea g una raíz primitiva módulo p . Si esta g es una raíz primitiva mod p^α para todo $\alpha \geq 1$ entonces, en particular, es una raíz primitiva mod p^2 y, como ya hemos indicado tendremos (5).

Veamos ahora el recíproco. Suponemos que g es una raíz primitiva mod p que satisface (5). Debemos demostrar que g también es una raíz primitiva mod p^α para todo $\alpha \geq 2$. Sea t el exponente de g mod p^α . Queremos ver que $t = \varphi(p^\alpha)$. Dado que $g^t \equiv 1 \pmod{p^\alpha}$ tenemos también $g^t \equiv 1 \pmod{p}$ luego $\varphi(p) | t$ y podemos escribir

$$(6) \quad t = q\varphi(p).$$

Ahora bien $t|\varphi(p^\alpha)$, luego $q\varphi(p)|\varphi(p^\alpha)$. Pero $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, luego

$$q(p-1)|p^{\alpha-1}(p-1)$$

que significa que $q|p^{\alpha-1}$. Por consiguiente $q = p^\beta$, en donde $\beta \leq \alpha - 1$, y (6) se transforma en

$$t = p^\beta(p-1).$$

Si demostramos que $\beta = \alpha - 1$ entonces $t = \varphi(p^\alpha)$ y la demostración estará terminada.

Suponemos, por el contrario, que $\beta < \alpha - 1$. Entonces $\beta \leq \alpha - 2$ y tenemos

$$t = p^\beta(p-1)|p^{\alpha-2}(p-1) = \varphi(p^{\alpha-1}).$$

Entonces, como $\varphi(p^{\alpha-1})$ es un múltiplo de t , esto implica,

$$(7) \quad g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}.$$

Ahora utilizamos el lema que sigue para demostrar que (7) es una contradicción. Esta contradicción completará la demostración del teorema 10.6. $\square$

Lema 2. Sea g una raíz primitiva módulo p tal que

$$(8) \quad g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Entonces, para cada $\alpha \geq 2$, tenemos

$$(9) \quad g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}.$$

DEMOSTRACIÓN DEL LEMA 2 Usamos inducción sobre α . Para $\alpha = 2$, la relación (9) se reduce a (8). Suponemos entonces que (9) se verifica para α . Por el teorema de Euler-Fermat tenemos

$$g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}$$

o sea

$$g^{\varphi(p^{\alpha-1})} = 1 + kp^{\alpha-1}$$

en donde $p \nmid k$ en virtud de (9). Elevando los dos miembros de la última igualdad a la potencia p obtenemos

$$g^{\varphi(p^\alpha)} = (1 + kp^{\alpha-1})^p = 1 + kp^\alpha + k^2 \frac{p(p-1)}{2} p^{2(\alpha-1)} + rp^{3(\alpha-1)}.$$

Ahora bien $2\alpha - 1 \geq \alpha + 1$ y $3\alpha - 3 \geq \alpha + 1$ ya que $\alpha \geq 2$. Luego la última ecuación proporciona la congruencia

$$g^{\varphi(p^\alpha)} \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}}$$

en donde $p \nmid k$. Con otras palabras, $g^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$ o sea que (9) se verifica para $\alpha + 1$, si se verifica para α . Esto termina la demostración del lema 2 y también la del teorema 10.6. $\square$

10.7 LA EXISTENCIA DE RAÍCES PRIMITIVAS mod $2p^\alpha$

Teorema 10.7 Si p es un primo impar y $\alpha \geq 1$ existen raíces primitivas impares módulo p^α . Cada una de tales g es también una raíz primitiva módulo $2p^\alpha$.

DEMOSTRACIÓN. Si g es una raíz primitiva módulo p^α también lo es $g + p^\alpha$. Pero bien g o $g + p^\alpha$ es impar, luego siempre existen raíces primitivas impares mod p^α . Sea g una raíz primitiva impar módulo p^α y sea f el exponente de g mod $2p^\alpha$. Debemos demostrar que $f = \varphi(2p^\alpha)$. Ahora bien $f \mid \varphi(2p^\alpha)$, y $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$, luego $f \mid \varphi(p^\alpha)$. Por otro lado, $g^f \equiv 1 \pmod{2p^\alpha}$, o sea que $g^f \equiv 1 \pmod{p^\alpha}$, luego $\varphi(p^\alpha) \mid f$ ya que g es una raíz primitiva mod p^α . Por consiguiente $f = \varphi(p^\alpha) = \varphi(2p^\alpha)$, luego g es una raíz primitiva mod $2p^\alpha$. $\square$

10.8 LA NO EXISTENCIA DE RAÍCES PRIMITIVAS EN LOS RESTANTES CASOS

Teorema 10.8 Dado $m \geq 1$ en donde m no es de la forma $m = 1, 2, 4, p^\alpha$, o $2p^\alpha$, en donde p es un primo impar, entonces para todo a con $(a, m) = 1$ tenemos

$$a^{\varphi(m)/2} \equiv 1 \pmod{m},$$

luego no existen raíces primitivas mod m .

DEMOSTRACIÓN. Hemos demostrado ya que no existen raíces primitivas mod 2^α si $\alpha \geq 3$. Por consiguiente podemos suponer que m admite la descomposición

$$m = 2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

en donde los p_i son primos impares, $s \geq 1$, y $\alpha \geq 0$. Dado que m no es de la forma 1, 2, 4, p o $2p^\alpha$ tenemos $\alpha \geq 2$ si $s = 1$ y $s \geq 2$ si $\alpha = 0$ ó 1. Obsérvese que

$$\varphi(m) = \varphi(2^\alpha) \varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}).$$

Sea ahora a un entero primo con m . Debemos probar que

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}.$$

Sea g una raíz primitiva mod $p_1^{\alpha_1}$ y elijamos k de forma que

$$a \equiv g^k \pmod{p_1^{\alpha_1}}.$$

Entonces tenemos

$$(10) \quad a^{\varphi(m)/2} \equiv g^{k\varphi(m)/2} \equiv g^{t\varphi(p_1^{\alpha_1})} \pmod{p_1^{\alpha_1}}$$

en donde

$$t = k\varphi(2^\alpha)\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})/2.$$

Probaremos que t es un entero. Si $\alpha \geq 2$, el factor $\varphi(2^\alpha)$ es par y entonces t es un entero. Si $\alpha = 0$ ó 1, entonces $s \geq 2$ y el factor $\varphi(p_2^{\alpha_2})$ es par, luego t es un entero también en este caso. Luego la congruencia (10) nos da

$$a^{\varphi(m)/2} \equiv 1 \pmod{p_1^{\alpha_1}}.$$

Del mismo modo obtenemos

$$(11) \quad a^{\varphi(m)/2} \equiv 1 \pmod{p_i^{\alpha_i}}$$

para cada $i = 1, 2, \dots, s$. Ahora probaremos que esta congruencia también se

verifica mod 2^α . Si $\alpha \geq 3$ la condición $(a, m) = 1$ requiere que a sea impar y podemos aplicar el teorema 10.3 para escribir

$$a^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}.$$

Como $\varphi(2^\alpha) | \varphi(m)$ esto nos proporciona

$$(12) \quad a^{\varphi(m)/2} \equiv 1 \pmod{2^\alpha}$$

para $\alpha \geq 3$.

Si $\alpha \leq 2$ tenemos

$$(13) \quad a^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}.$$

Pero $s \geq 1$, luego $\varphi(m) = \varphi(2^s) \varphi(p_1^{\alpha_1}) \dots \varphi(p_s^{\alpha_s}) = 2r\varphi(2^\alpha)$, en donde r es un entero. Luego $\varphi(2^\alpha) | \varphi(m)/2$ y (13) implica (12) para $\alpha \leq 2$. Luego (12) se verifica para todo α . Multiplicando las congruencias (11) y (12) obtenemos

$$a^{\varphi(m)/2} \equiv 1 \pmod{m},$$

y ello demuestra que a no puede ser una raíz primitiva mod m . □

10.9 EL NÚMERO DE RAÍCES PRIMITIVAS mod m

Hemos demostrado que un entero $m \geq 1$ tiene una raíz primitiva si, y sólo si,

$$m = 1, 2, 4, p^\alpha \text{ o } 2p^\alpha,$$

en donde p es un primo impar y $\alpha \geq 1$. El teorema que sigue nos dice cuántas raíces primitivas existen para cada m .

Teorema 10.9 *Si m tiene una raíz primitiva g entonces m tiene exactamente $\varphi(\varphi(m))$ raíces primitivas incongruentes y están dadas por los números del conjunto.*

$$S = \{g^n : 1 \leq n \leq \varphi(m), \text{ y } (n, \varphi(m)) = 1\}.$$

DEMOSTRACIÓN. Tenemos $\exp_m(g) = \varphi(m)$, y el lema 1 prueba que $\exp_m(g^n) = \exp_m(g)$ si, y sólo si, $(n, \varphi(m)) = 1$. Por consiguiente cada elemento de S es una raíz primitiva mod m .

Recíprocamente, si a es una raíz primitiva mod m , entonces $a \equiv g^k \pmod{m}$ para algún $k = 1, 2, \dots, \varphi(m)$. Luego $\exp_m(g^k) = \exp_m(a) = \varphi(m)$, y el lema 1 im-

plica $(k, \varphi(m)) = 1$. Por consiguiente cada raíz primitiva es un elemento de S . Puesto que S contiene $\varphi(\varphi(m))$ elementos no congruentes mod m la demostración queda establecida. $\square$

Aunque hemos demostrado la existencia de raíces primitivas para ciertos módulos, no se conoce ningún método directo para calcular tales raíces, de forma

Tabla 10.1 $g(p)$ es la menor raíz primitiva del primo p

p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$	p	$g(p)$
2	1	109	6	269	2	439	15	617	3	811	3
3	2	113	3	271	6	443	2	619	2	821	2
5	2	127	3	277	5	449	3	631	3	823	3
7	3	131	2	281	3	457	13	641	3	827	2
11	2	137	3	283	3	461	2	643	11	829	2
13	2	139	2	293	2	463	3	647	5	839	11
17	3	149	2	307	5	467	2	653	2	853	2
19	2	151	6	311	17	479	13	659	2	857	3
23	5	157	5	313	10	487	3	661	2	859	2
29	2	163	2	317	2	491	2	673	5	863	5
31	3	167	5	331	3	499	7	677	2	877	2
37	2	173	2	337	10	503	5	683	5	881	3
41	6	179	2	347	2	509	2	691	3	883	2
43	3	181	2	349	2	521	3	701	2	887	5
47	5	191	19	353	3	523	2	709	2	907	2
53	2	193	5	359	7	541	2	719	11	911	17
59	2	197	2	367	6	547	2	727	5	919	7
61	2	199	3	373	2	557	2	733	6	929	3
67	2	211	2	379	2	563	2	739	3	937	5
71	7	223	3	383	5	569	3	743	5	941	2
73	5	227	2	389	2	571	3	751	3	947	2
79	3	229	6	397	5	577	5	757	2	953	3
83	2	233	3	401	3	587	2	761	6	967	5
89	3	239	7	409	21	593	3	769	11	971	6
97	5	241	7	419	2	599	7	773	2	977	3
101	2	251	6	421	2	601	7	787	2	983	5
103	5	257	3	431	7	607	3	797	2	997	7
107	2	263	5	433	5	613	2	809	3		

general, sin efectuar gran cantidad de cálculos, especialmente para módulos grandes. Si $g(p)$ designa la menor raíz primitiva mod p , la tabla 10.1 da una lista de $g(p)$ para todos los primos < 1000 .

10.10 CÁLCULO DE ÍNDICES

Si m tiene una raíz primitiva g , los números $1, g, g^2, \dots, g^{\varphi(m)-1}$ forma un sistema residual reducido mod m . Si $(a, m) = 1$ existe un único entero k en el intervalo $0 \leq k \leq \varphi(m) - 1$ tal que

$$a \equiv g^k \pmod{m}.$$

Este entero se llama *índice* de a en base $g \pmod{m}$, y escribimos

$$k = \text{ind}_g a$$

o simplemente $k = \text{ind } a$ cuando la base g se sobrentiende.

El teorema que sigue prueba que los índices tienen propiedades análogas a las de los logaritmos. La demostración se deja como ejercicio para el lector.

Teorema 10.10 Sea g una raíz primitiva mod m . Si $(a, m) = (b, m) = 1$ tenemos:

- (a) $\text{ind}(ab) = \text{ind } a + \text{ind } b \pmod{\varphi(m)}$.
- (b) $\text{ind } g^n \equiv n \text{ ind } a \pmod{\varphi(m)}$ si $n \geq 1$.
- (c) $\text{ind } 1 = 0$ e $\text{ind } g = 1$.
- (d) $\text{ind}(-1) = \varphi(m)/2$ si $m > 2$.
- (e) Si g' es también una raíz primitiva mod m entonces

$$\text{ind}_g a \equiv \text{ind}_{g'} a \cdot \text{ind}_{g'} g' \pmod{\varphi(m)}.$$

La tabla 10.2 de las pp. 268-269 da los índices para todos los números $a \not\equiv 0 \pmod{p}$ y para todos los primos $p < 50$. La base g es la menor raíz primitiva de p .

Los siguientes ejemplos ilustran el uso de índices para resolver congruencias.

EJEMPLO 1 Congruencias lineales. Suponemos que m tiene una raíz primitiva y que $(a, m) = (b, m) = 1$. Entonces la congruencia lineal

$$(14) \quad ax \equiv b \pmod{m}$$

es equivalente a la congruencia

Tabla 10.2 Índices de todos los números $a \not\equiv 0 \pmod{p}$ para primos impares $p < 50$. La base g es la menor raíz primitiva de p

a	Primos 3 5 7 11 13 17 19 23 29 31 37 41 43 47													
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37

21		13	17	29	22	14	36	6
22		11	26	17	31	29	15	25
23			20	27	15	36	16	5
24			8	13	29	13	40	28
25			16	10	10	4	8	2
26			19	5	12	17	17	29
27			15	3	6	5	3	14
28			14	16	34	11	5	22
29				9	21	7	41	35
30				15	14	23	11	39
31					9	28	34	3
32					5	10	9	44
33					20	18	31	27
34					8	19	23	34
35					19	21	18	33
36					18	2	14	30
37						32	7	42
38						35	4	17
39						6	33	31
40						20	22	9
41							6	15
42							21	24
43								13
44								43
45								41
46								23

$$\text{ind } a + \text{ind } x \equiv \text{ind } b \pmod{\varphi(m)},$$

luego la única solución de (14) satisface la congruencia

$$\text{ind } x \equiv \text{ind } b - \text{ind } a \pmod{\varphi(m)}.$$

Para efectuar un ejemplo numérico, consideremos la congruencia lineal

$$9x \equiv 13 \pmod{47}.$$

La correspondiente relación entre índices es

$$\text{ind } x \equiv \text{ind } 13 - \text{ind } 9 \pmod{46}.$$

De la tabla 10.2 obtenemos $\text{ind } 13 = 11$ e $\text{ind } 9 = 40$ (para $p = 47$), luego

$$\text{ind } x \equiv 11 - 40 \equiv -29 \equiv 17 \pmod{46}.$$

De nuevo recurriendo a la tabla 10.2 obtenemos $x \equiv 38 \pmod{47}$.

EJEMPLO 2 Congruencias binomiales. Una congruencia de la forma

$$x^n \equiv a \pmod{m}$$

se llama *congruencia binomial*. Si m tiene una raíz primitiva y si $(a, m) = 1$ ésta es equivalente a la congruencia

$$n \text{ ind } x \equiv \text{ind } a \pmod{\varphi(m)},$$

que es lineal en la incógnita $\text{ind } x$. Como tal tiene solución si, y sólo si, $\text{ind } a$ es divisible por $d = (n, \varphi(m))$, en cuyo caso tiene exactamente d soluciones.

Para ilustrarlo con un ejemplo numérico, consideramos la congruencia binomial

$$(15) \quad x^8 \equiv a \pmod{17}.$$

La relación con índices que le corresponde es

$$(16) \quad 8 \text{ ind } x \equiv \text{ind } a \pmod{16}.$$

En este ejemplo $d = (8, 16) = 8$. La tabla 10.2 prueba que 1 y 16 son los únicos

números mod 17 cuyo índice es divisible por 8. En efecto, $\text{ind } 1 = 0$ e $\text{ind } 16 = 8$. Luego (15) carece de solución si $a \not\equiv 1$ o $a \not\equiv 16 \pmod{17}$.

Para $a = 1$, la congruencia (16) se transforma en

$$(17) \quad 8 \text{ ind } x \equiv 0 \pmod{16},$$

y para $a = 16$ se transforma en

$$(18) \quad 8 \text{ ind } x \equiv 8 \pmod{16}.$$

Cada una de ellas tiene exactamente ocho soluciones mod 16. Las soluciones de (17) son los x cuyo índice es par,

$$x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}.$$

Éstos, además, son los restos cuadráticos de 17. Las soluciones de (18) son los x cuyo índice es impar; son los no restos cuadráticos de 17,

$$x \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}.$$

EJEMPLO 3 Congruencias exponenciales. Una congruencia exponencial es una congruencia de la forma

$$a^x \equiv b \pmod{m}.$$

Si m admite una raíz primitiva y si $(a, m) = (b, m) = 1$, es equivalente a la congruencia lineal

$$(19) \quad x \text{ ind } a \equiv \text{ind } b \pmod{\varphi(m)}.$$

Sea $d = (\text{ind } a, \varphi(m))$. Entonces (19) tiene una solución si, y sólo si, $d \mid \text{ind } b$, en cuyo caso existen exactamente d soluciones. En el ejemplo numérico

$$(20) \quad 25^x \equiv 17 \pmod{47}$$

tenemos $\text{ind } 25 = 2$, $\text{ind } 17 = 16$, y $d = (2, 46)$. Por consiguiente (19) se transforma en

$$2x \equiv 16 \pmod{46},$$

con dos soluciones, $x \equiv 8$ y $31 \pmod{46}$. Éstas son también las soluciones de (20) mod 47.

10.11 RAÍCES PRIMITIVAS Y CARACTERES DE DIRICHLET

Las raíces primitivas y los índices se pueden utilizar para construir explícitamente todos los caracteres de Dirichlet mod m . En primer lugar el módulo considerado es la potencia p^α de un primo p impar y $\alpha \geq 1$.

Sea g una raíz primitiva mod p que sea también raíz primitiva mod p^β para todo $\beta \geq 1$. Tales g existen en virtud del teorema 10.6. Si $(n, p) = 1$, sea $b(n) = \text{ind}_n n \pmod{p^\alpha}$ así que $b(n)$ es el único entero que satisface las condiciones

$$n \equiv g^{b(n)} \pmod{p^\alpha}, \quad 0 \leq b(n) < \varphi(p^\alpha).$$

Para $h = 0, 1, 2, \dots, \varphi(p^\alpha) - 1$, definimos χ_h por las relaciones

$$(21) \quad \chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)} & \text{si } p \nmid n, \\ 0 & \text{si } p \mid n. \end{cases}$$

Utilizando las propiedades de los índices es fácil comprobar que χ_h es completamente multiplicativa y periódica con período p^α , luego χ_h es un carácter de Dirichlet mod p^α , y χ_0 es el carácter principal. La comprobación se deja como ejercicio para el lector.

Como

$$\chi_h(g) = e^{2\pi i h/\varphi(p^\alpha)}$$

los caracteres $\chi_0, \chi_1, \dots, \chi_{\varphi(p^\alpha)-1}$ son distintos ya que toman distintos valores en g . Por consiguiente dado que existen $\varphi(p^\alpha)$ de estas funciones, representan todos los caracteres de Dirichlet mod p^α . La misma construcción vale para mod 2^α si $\alpha = 1$ ó 2 , utilizando $g = 3$ como raíz primitiva.

Ahora si $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ en donde los p_i son primos impares distintos, y si χ_i es un carácter de Dirichlet mod $p_i^{\alpha_i}$, entonces el producto $\chi = \chi_1 \dots \chi_r$ es un carácter de Dirichlet mod m . Como $\varphi(m) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$ obtenemos $\varphi(m)$ de tales caracteres cuando cada χ_i recorre los $\varphi(p_i^{\alpha_i})$ caracteres mod $p_i^{\alpha_i}$. Luego tenemos contruidos explícitamente todos los caracteres mod m para cada módulo impar m .

Si $\alpha \geq 3$, el módulo 2^α carece de raíces primitivas y necesitamos una construcción ligeramente diferente para obtener los caracteres mod 2^α . El teorema que sigue demuestra que 5 es un buen sustituto para una raíz primitiva mod 2^α .

Teorema 10.11 *Suponemos $\alpha \geq 3$. Entonces, para cada entero impar n , existe un entero $b(n)$, unívocamente determinado, tal que*

$$n \equiv (-1)^{(n-1)/2} 5^{b(n)} \pmod{2^\alpha}, \text{ con } 1 \leq b(n) \leq \varphi(2^\alpha)/2.$$

DEMOSTRACIÓN. Sea $f = \exp_{2^\alpha}(5)$ o sea que $5^f \equiv 1 \pmod{2^\alpha}$. Probaremos que $f = \varphi(2^\alpha)/2$. Ahora bien $f | \varphi(2^\alpha) = 2^{\alpha-1}$, luego $f = 2^\beta$ para algún $\beta \leq \alpha - 1$. Del teorema 10.8 deducimos

$$5^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha},$$

luego $f \leq \varphi(2^\alpha)/2 = 2^{\alpha-2}$. Por consiguiente $\beta \leq \alpha - 2$. Probaremos que $\beta = \alpha - 2$.

Si elevamos los dos miembros de la igualdad $5 = 1 + 2^2$ a la potencia $f = 2^\beta$ obtenemos

$$5^f = (1 + 2^2)^{2^\beta} = 1 + 2^{\beta+2} + r2^{\beta+3} = 1 + 2^{\beta+2}(1 + 2r)$$

en donde r es un entero. Luego $5^f - 1 = 2^{\beta+2}t$, en donde t es impar. Pero $2^\alpha | (5^f - 1)$ por lo que $\alpha \leq \beta + 2$, o bien $\beta \geq \alpha - 2$. Luego $\beta = \alpha - 2$ y $f = 2^{\alpha-2} = \varphi(2^\alpha)/2$. Por consiguiente los números

$$(22) \quad 5, 5^2, \dots, 5^f$$

son incongruentes mod 2^α . También cada uno de ellos es $\equiv 1 \pmod{4}$ ya que $5 \equiv 1 \pmod{4}$. Análogamente los números

$$(23) \quad -5, -5^2, \dots, -5^f$$

son incongruentes mod 2^α y cada uno de ellos es $\equiv 3 \pmod{4}$ ya que $-5 \equiv 3 \pmod{4}$. Existen $2f = \varphi(2^\alpha)$ números en (22) y (23) conjuntamente. Además no es posible que $5^a \equiv -5^b \pmod{2^\alpha}$ ya que ello implicaría $1 \equiv -1 \pmod{4}$. Luego los números de (22) junto con los de (23) representan $\varphi(2^\alpha)$ números impares incongruentes mod 2^α . Cada impar $n \equiv 1 \pmod{4}$ es congruente mod 2^α a uno de los números de (22), y cada impar $n \equiv 3 \pmod{4}$ es congruente con uno de (23). Esto prueba el teorema. $\square$

Con la ayuda del teorema 10.11 podemos construir todos los caracteres mod 2^α si $\alpha \geq 3$. Sea

$$(24) \quad f(n) = \begin{cases} (-1)^{(n-1)/2} & \text{si } n \text{ es impar,} \\ 0 & \text{si } n \text{ es par,} \end{cases}$$

y sea

$$g(n) = \begin{cases} e^{2\pi i b(n)/2^{a-2}} & \text{si } n \text{ es impar,} \\ 0 & \text{si } n \text{ es par,} \end{cases}$$

en donde $b(n)$ es el entero proporcionado por el teorema 10.11. Entonces es fácil comprobar que cada uno de los f y de los g es un carácter mod 2^a . Luego también lo es cada producto

$$(25) \quad \chi_{a,c}(n) = f(n)^a g(n)^c$$

en donde $a = 1, 2$, y $c = 1, 2, \dots, \varphi(2^a)/2$. Además, estos $\varphi(2^a)$ caracteres son distintos, luego representan todos los caracteres mod 2^a .

Ahora, si $m = 2^a Q$ en donde Q es impar, formamos los productos $\chi = \chi_1 \chi_2$, en donde χ_1 recorre los $\varphi(2^a)$ caracteres mod 2^a y χ_2 recorre los $\varphi(Q)$ caracteres mod Q para obtener todos los caracteres mod m .

10.12 CARACTERES DE DIRICHLET mod p^a CON VALORES REALES

Si χ es un carácter de Dirichlet mod m con valores reales y $(n, m) = 1$, el número $\chi(n)$ es a la vez una raíz de la unidad y es real, luego $\chi(n) = \pm 1$. Por la construcción de la sección anterior podemos determinar todos los caracteres de Dirichlet mod p^a con valores reales.

Teorema 10.12 *Para un primo p impar y $\alpha \geq 1$, consideremos los $\varphi(p^\alpha)$ caracteres de Dirichlet χ_h mod p^α dados por (21). Entonces χ_h es real si, y sólo si, $h = 0$ o $h = \varphi(p^\alpha)/2$. Luego existen exactamente dos caracteres reales mod p^α .*

DEMOSTRACIÓN. Tenemos $e^{\pi iz} = \pm 1$ si, y sólo si, z es un entero. Si $p \nmid n$ tenemos

$$\chi_h(n) = e^{2\pi i h b(n)/\varphi(p^\alpha)}$$

luego $\chi_h(n) = \pm 1$ si, y sólo si, $\varphi(p^\alpha) | 2hb(n)$. Esta condición la satisface todo n si $h = 0$ o si $h = \varphi(p^\alpha)/2$. Recíprocamente, si $\varphi(p^\alpha) | 2hb(n)$ para todo n entonces cuando

$b(n) = 1$ tenemos $\varphi(p^\alpha) \mid 2h$ o $\varphi(p^\alpha)/2 \mid h$. Luego $h = 0$ o $h = \varphi(p^\alpha)/2$ ya que éstos son los únicos múltiplos de $\varphi(p^\alpha)/2$ menores que $\varphi(p^\alpha)$. $\square$

Nota. El carácter que corresponde a $h = 0$ es el carácter principal. Cuando $\alpha = 1$ el carácter cuadrático $\chi(n) = (n|p)$ es el otro carácter real mod p .

Para los módulos $m = 1, 2$, y 4 , todos los caracteres de Dirichlet son reales. El teorema que sigue describe los caracteres reales mod 2^α cuando $\alpha \geq 3$.

Teorema 10.13 Si $\alpha \geq 3$, consideramos los $\varphi(2^\alpha)$ caracteres de Dirichlet $\chi_{a,c}$ mod 2^α dados por (25). Entonces $\chi_{a,c}$ es real si, y sólo si, $c = \varphi(2^\alpha)/2$ ó $c = \varphi(2^\alpha)/4$. Luego hay exactamente cuatro caracteres reales mod 2^α si $\alpha \geq 3$.

DEMOSTRACIÓN. Si $\alpha \geq 3$ y n es impar tenemos, por (25),

$$\chi_{a,c}(n) = f(n)^a g(n)^c$$

en donde $f(n) = \pm 1$ y

$$g(n)^c = e^{2\pi i c b(n)/2^{\alpha-2}},$$

con $1 \leq c \leq 2^{\alpha-2}$. Esto es ± 1 si, y sólo si, $2^{\alpha-2} \mid 2cb(n)$, ó $2^{-3} \mid cb(n)$. Puesto que $\varphi(2^\alpha) = 2^{\alpha-1}$ esta condición se verifica si $c = \varphi(2^\alpha)/2 = 2^{\alpha-2}$ o si $c = \varphi(2^\alpha)/4 = 2^{\alpha-3}$. Recíprocamente, si $2^{\alpha-3} \mid cb(n)$ para todo n entonces $b(n) = 1$ requiere que $2^{\alpha-3} \mid c$ o sea que $c = 2^{\alpha-3}$ ó $2^{\alpha-2}$ ya que $1 \leq c \leq 2^{\alpha-2}$. $\square$

10.13 CARACTERES DE DIRICHLET PRIMITIVOS mod p^α

En el teorema 8.14 probábamos que cada carácter no principal χ mod p es primitivo si p es primo. Ahora determinaremos todos los caracteres de Dirichlet primitivos mod p^α .

Recordemos (sección 8.7) que χ es primitivo mod k si, y sólo si, χ carece de módulo inducido $d < k$. Un módulo inducido es un divisor d de k tal que

$$\chi(n) = 1 \quad \text{si } (n, k) = 1 \text{ y } n \equiv 1 \pmod{d}.$$

Si $k = p^\alpha$ y χ es no primitivo mod p^α entonces uno de los divisores $1, p, \dots, p^{\alpha-1}$ es un módulo inducido y por tanto $p^{\alpha-1}$ es un módulo inducido. Por consiguiente, χ es primitivo mod p^α si, y sólo si, $p^{\alpha-1}$ no es un módulo inducido para χ .

Teorema 10.14 Para un primo impar p y $\alpha \geq 2$, consideramos los $\varphi(p^\alpha)$ caracteres de Dirichlet $\chi_h \bmod p^\alpha$ dados por (21). Entonces χ_h es primitivo mod p^α si, y sólo si, $p \nmid h$.

DEMOSTRACIÓN. Probaremos que $p^{\alpha-1}$ es un módulo inducido si, y sólo si, $p|h$. Si $p \nmid h$ tenemos, por (21),

$$\chi_h(n) = e^{2\pi i h b(n)/\varphi(p^\alpha)},$$

en donde $n \equiv g^{b(n)} \pmod{p^\alpha}$ y g es una raíz primitiva mod p^β para todo $\beta \geq 1$. Por consiguiente

$$g^{b(n)} \equiv n \pmod{p^{\alpha-1}}.$$

Ahora si $n \equiv 1 \pmod{p^{\alpha-1}}$ entonces $g^{b(n)} \equiv 1 \pmod{p^{\alpha-1}}$ y, como g es una raíz primitiva de $p^{\alpha-1}$, tenemos $\varphi(p^{\alpha-1})|b(n)$, luego

$$b(n) = t\varphi(p^{\alpha-1}) = t\varphi(p^\alpha)/p$$

para un entero t . Por lo tanto

$$\chi_h(n) = e^{2\pi i h t/p}.$$

Si $p|h$, esto es igual a 1 y por lo tanto χ_h no es primitivo mod p^α . Si $p \nmid h$ tomamos $n = 1 + p^{\alpha-1}$. Entonces $n \equiv 1 \pmod{p^{\alpha-1}}$ pero $n \not\equiv 1 \pmod{p^\alpha}$ o sea que $0 < b(n) < \varphi(p^\alpha)$. Por consiguiente $p \nmid t$, $p \nmid ht$ y $\chi_h(n) \neq 1$. Esto demuestra que χ_h es primitivo si $p \nmid h$. $\square$

Cuando $m = 1$ ó 2 , existe un único carácter $\chi \bmod m$, el carácter principal. Si $m = 4$ existen dos caracteres mod 4, el carácter principal y el carácter primitivo f dado por (24). El teorema que sigue describe todos los caracteres primitivos mod 2^α para $\alpha \geq 3$. La demostración es análoga a la del teorema 10.14 y se deja como ejercicio al lector.

Teorema 10.15 Si $\alpha \geq 3$, consideramos los $\varphi(2^\alpha)$ caracteres de Dirichlet $\chi_{a,c}$ mod 2^α dados por (25). Entonces $\chi_{a,c}$ es primitivo mod 2^α si, y sólo si, c es impar.

Los resultados precedentes describen todos los caracteres primitivos mod p^α para todas las potencias de primos. Para determinar los caracteres primitivos para módulos compuestos k escribimos

$$k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Entonces cada carácter $\chi \bmod k$ se descompone en la forma

$$\chi = \chi_1 \cdots \chi_r$$

en donde cada χ_i es un carácter mod $p_i^{a_i}$. Además, por el ejercicio 8.12, χ es primitivo mod k si, y sólo si, cada χ_i es primitivo mod $p_i^{a_i}$. Por consiguiente tenemos una descripción completa de todos los caracteres primitivos mod k .

Ejercicios del capítulo 10

1. Probar que m es primo si, y sólo si, $\exp_m(a) = m - 1$ para algún a .
2. Si $(a, m) = (b, m) = 1$ y si $(\exp_m(a), \exp_m(b)) = 1$, probar que

$$\exp_m(ab) = \exp_m(a)\exp_m(b).$$

3. Sea g una raíz primitiva de un primo impar p . Probar que $-g$ también es una raíz primitiva de p si $p \equiv 1 \pmod{4}$, pero que $\exp_p(-g) = (p-1)/2$ si $p \equiv 3 \pmod{4}$.
4. (a) Probar que 3 es una raíz primitiva mod p si p es un primo de la forma $2^n + 1$, $n > 1$.
(b) Probar que 2 es una raíz primitiva mod p si p es un primo de la forma $4q + 1$, en donde q es un primo impar.
5. Sea $m > 2$ un entero con una raíz primitiva, y sea $(a, m) = 1$. Escribiremos aRm si existe un x tal que $a \equiv x^2 \pmod{m}$. Probar que:
(a) aRm si, y sólo si, $a^{\varphi(m)/2} \equiv 1 \pmod{m}$.
(b) Si aRm , la congruencia $x^2 \equiv a \pmod{m}$ tiene exactamente dos soluciones.
(c) Existen exactamente $\varphi(m)/2$ enteros a , incongruentes mod m , tales que $(a, m) = 1$ y aRm .
6. Suponemos $m > 2$, $(a, m) = 1$, aRm . Probar que la congruencia $x^2 \equiv a \pmod{m}$ tiene exactamente dos soluciones si, y sólo si, m tiene una raíz primitiva.
7. Sea $S_n(p) = \sum_{k=1}^{p-1} k^n$, en donde p es un impar y $n > 1$. Probar que

$$S_n(p) \equiv \begin{cases} 0 \pmod{p} & \text{si } n \not\equiv 0 \pmod{p-1}, \\ -1 \pmod{p} & \text{si } n \equiv 0 \pmod{p-1}. \end{cases}$$

8. Probar que la suma de las raíces primitivas mod p es congruente con $\mu(p-1) \pmod{p}$.
9. Si p es un primo impar > 3 , probar que el producto de las raíces primitivas mod p es congruente con $1 \pmod{p}$.
10. Sea p un primo impar de la forma $2^{2^k} + 1$. Probar que el conjunto de las raíces primitivas mod p es igual al conjunto de los no restos cuadráticos mod p . Utilizar este resultado para probar que 7 es una raíz primitiva de cada uno de estos primos.
11. Suponemos que $d | \varphi(m)$. Si $d = \exp_m(a)$ decimos que a es una raíz primitiva de la congruencia

$$x^d \equiv 1 \pmod{m}.$$

Probar que si la congruencia

$$x^{\varphi(m)} \equiv 1 \pmod{m}$$

tiene una raíz primitiva entonces tiene $\varphi(\varphi(m))$ raíces primitivas, incongruentes mod m .

12. Probar las propiedades de los índices descritas en el teorema 10.10.
 13. Sea p un primo impar. Si $(h, p) = 1$ sea

$$S(h) = \{h^n: 1 \leq n \leq \varphi(p-1), (n, p-1) = 1\}.$$

- Si h es una raíz primitiva de p , los números del conjunto $S(h)$ son distintos mod p (son de hecho, las raíces primitivas de p). Probar que existe un entero h , que no es raíz primitiva de p , tal que los números de $S(h)$ son distintos mod p si, y sólo si, $p \equiv 3 \pmod{4}$.
14. Si $m > 1$, sean $p_1, \dots, p_k$ divisores primos distintos de $\varphi(m)$. Si $(g, m) = 1$, probar que g es una raíz primitiva de m si, y sólo si, g no satisface ninguna de las congruencias $g^{\varphi(m)/p_i} \equiv 1 \pmod{m}$ para $i = 1, 2, \dots, k$.
15. El primo $p = 71$ tiene 7 raíces primitivas. Buscar todas las raíces primitivas de 71 y también una raíz primitiva de p^2 y de $2p^2$.
16. Resolver cada una de las congruencias siguientes:
- $8x \equiv 7 \pmod{43}$.
 - $x^8 \equiv 17 \pmod{43}$.
 - $8^x \equiv 3 \pmod{43}$.
17. Sea q un primo impar y sea $p = 4q + 1$ también primo.
- Probar que la congruencia $x^2 \equiv -1 \pmod{p}$ tiene exactamente dos soluciones, y que cada una de ellas es un no resto cuadrático de p .
 - Probar que cada no resto cuadrático de p es una raíz primitiva de p , con la excepción de los dos no restos de (a).
 - Hallar todas las raíces primitivas de 29.
18. (Extensión del ejercicio 17.) Sea q un primo impar y supongamos que $p = 2^n q + 1$ es primo. Probar que cada no resto cuadrático a de p es una raíz primitiva de p si $a^{2^n} \not\equiv 1 \pmod{p}$.
19. Probar que sólo existen dos caracteres reales primitivos mod 8 y construir una tabla que dé sus valores.
20. Sea χ un carácter real primitivo mod m . Si m no es una potencia de 2 probar que m tiene la forma

$$m = 2^\alpha p_1 \cdots p_r$$

en donde los p_i son primos distintos impares y $\alpha = 0, 2$ ó 3 . Si $\alpha = 0$ probar que

$$\chi(-1) = \prod_{p|m} (-1)^{(p-1)/2}$$

y hallar una fórmula análoga para $\chi(-1)$ cuando $\alpha = 2$.

Capítulo 11

Series de Dirichlet y productos de Euler

11.1 INTRODUCCIÓN

En 1737 Euler demostró el teorema de Euclides relativo a la existencia de una infinidad de números primos viendo que la serie $\sum p^{-1}$, extendida a todos los números primos, diverge. Este resultado lo dedujo del hecho de que la función zeta $\zeta(s)$, dada por

$$(1) \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

para valores reales $s > 1$, tiende a ∞ cuando $s \rightarrow 1$. En 1837, Dirichlet demostró su célebre teorema relativo a los primos existentes en una progresión aritmética estudiando la serie

$$(2) \quad L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

en donde χ es un carácter de Dirichlet y $s > 1$.

Las series (1) y (2) son ejemplos de series de la forma

$$(3) \quad \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

en donde $f(n)$ es una función aritmética. Estas series reciben el nombre de series de Dirichlet de coeficientes $f(n)$. Estas series constituyen una de las herramientas más útiles de la Teoría analítica de números.

Este capítulo estudia las propiedades generales de las series de Dirichlet. El capítulo siguiente efectúa un estudio más detallado de la función zeta de Riemann $\zeta(s)$ y de las L -funciones de Dirichlet $L(s, \chi)$.

Notación. De acuerdo con Riemann, sea s una variable compleja y escribamos

$$s = \sigma + it,$$

en donde σ y t son reales. Entonces $n^s = e^{s \log n} = e^{(\sigma+it) \log n} = n^\sigma e^{it \log n}$. Esto prueba que $|n^s| = n^\sigma$ puesto que $|e^{i\theta}| = 1$ para θ real.

El conjunto de puntos $s = \sigma + it$ tales que $\sigma > a$ se llama *semiplano*. Demostremos que, para cada serie de Dirichlet, existe un semiplano $\sigma > \sigma_c$ en el que la serie converge, y otro semiplano $\sigma > \sigma_a$ en el que converge absolutamente. Probaremos además que, en el semiplano de convergencia, la serie representa una función analítica de la variable compleja s .

11.2 EL SEMIPLANO DE CONVERGENCIA ABSOLUTA DE UNA SERIE DE DIRICHLET

Observemos en primer lugar que, si $\sigma \geq a$, tenemos $|n^s| = n^\sigma \geq n^a$, por lo tanto

$$\left| \frac{f(n)}{n^s} \right| \leq \frac{|f(n)|}{n^a}.$$

Por consiguiente, si una serie de Dirichlet $\sum f(n)n^{-s}$ converge absolutamente para $s = a + ib$, entonces, por el criterio de comparación, converge también absolutamente para todo s con $\sigma \geq a$.

Teorema 11.1 *Supongamos que la serie $\sum |f(n)n^{-s}|$ ni converge para todo s ni diverge para todo s . Entonces existe un número real σ_a , llamado abscisa de convergencia absoluta, tal que la serie $\sum f(n)n^{-s}$ converge absolutamente si $\sigma > \sigma_a$ pero, en cambio, no converge absolutamente, si $\sigma < \sigma_a$.*

DEMOSTRACIÓN. Sea D el conjunto de todos los números reales σ tales que $\sum |f(n)n^{-s}|$ diverge. D es no vacío puesto que esta serie no converge para todo s , y D está acotado superiormente ya que la serie no diverge para todo s . Por consiguiente

D admite un supremo que llamaremos σ_a . Si $\sigma < \sigma_a$, entonces $\sigma \in D$, en otro caso σ sería una cota superior de D menor que su supremo. Si $\sigma > \sigma_a$, entonces $\sigma \notin D$ puesto que σ_a es el supremo de D . Esto demuestra el teorema. $\square$

Nota. Si $\sum |f(n)n^{-s}|$ converge para todo real, definimos $\sigma_a = -\infty$. Si la serie $\sum |f(n)n^{-s}|$ no converge para ningún s , definimos $\sigma_a = +\infty$.

EJEMPLO 1 Función zeta de Riemann. La serie de Dirichlet $\sum_{n=1}^{\infty} n^{-s}$ converge absolutamente para $\sigma > 1$. Cuando $s = 1$ la serie diverge, por lo tanto $\sigma_a = 1$. La suma de esta serie se designa $\zeta(s)$ y se llama función zeta de Riemann.

EJEMPLO 2 Si f está acotada, o sea si $|f(n)| \leq M$ para todo $n \geq 1$, entonces $\sum f(n)n^{-s}$ converge absolutamente para $\sigma > 1$, luego $\sigma_a \leq 1$. En particular, si χ es un carácter de Dirichlet, la L -serie $L(s, \chi) = \sum \chi(n)n^{-s}$ converge absolutamente para $\sigma > 1$.

EJEMPLO 3 La serie $\sum n^n n^{-s}$ diverge para cada s , luego $\sigma_a = +\infty$.

EJEMPLO 4 La serie $\sum n^{-n} n^{-s}$ converge absolutamente para todo s , luego $\sigma_a = -\infty$.

11.3 LA FUNCIÓN DEFINIDA POR UNA SERIE DE DIRICHLET

Suponemos que $\sum f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$ y consideramos la función suma $F(s)$:

$$(4) \quad F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{para } \sigma > \sigma_a.$$

En esta sección se obtienen algunas de las propiedades de $F(s)$. En primer lugar se demuestra el lema que sigue.

Lema 1 Si $N \geq 1$ y $\sigma \geq c > \sigma_a$ tenemos

$$\left| \sum_{n=N}^{\infty} f(n)n^{-s} \right| \leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)|n^{-c}.$$

DEMOSTRACIÓN. Tenemos

$$\begin{aligned} \left| \sum_{n=N}^{\infty} f(n)n^{-s} \right| &\leq \sum_{n=N}^{\infty} |f(n)|n^{-\sigma} = \sum_{n=N}^{\infty} |f(n)|n^{-c}n^{-(\sigma-c)} \\ &\leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)|n^{-c}. \end{aligned} \quad \square$$

El teorema que sigue describe el comportamiento de $F(s)$ cuando $\sigma \rightarrow +\infty$.

Teorema 11.2 Si $F(s)$ está definida por (4), entonces

$$\lim_{\sigma \rightarrow +\infty} F(\sigma + it) = f(1)$$

uniformemente para $-\infty < t < +\infty$.

DEMOSTRACIÓN. Puesto que $F(s) = f(1) + \sum_{n=2}^{\infty} f(n)n^{-s}$, únicamente debemos demostrar que el segundo término tiende a 0 cuando $\sigma \rightarrow +\infty$. Elegimos $c > \sigma_a$. Entonces para $\sigma \geq c$ el lema implica

$$\left| \sum_{n=2}^{\infty} \frac{f(n)}{n^s} \right| \leq 2^{-(\sigma-c)} \sum_{n=2}^{\infty} |f(n)|n^{-c} = \frac{A}{2^\sigma}$$

en donde A es independiente de σ y de t . Dado que $A/2^\sigma \rightarrow 0$ cuando $\sigma \rightarrow +\infty$ el teorema queda establecido. $\square$

EJEMPLOS $\zeta(\sigma + it) \rightarrow 1$ y $L(\sigma + it, \chi) \rightarrow 1$ cuando $\sigma \rightarrow +\infty$.

A continuación vemos que todos los coeficientes están unívocamente determinados por la función suma.

Teorema 11.3 Teorema de unicidad. Dadas dos series de Dirichlet

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{y} \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s},$$

ambas absolutamente convergentes para $\sigma > \sigma_a$. Si $F(s) = G(s)$ para cada s de una sucesión infinita $\{s_k\}$ tal que $\sigma_k \rightarrow +\infty$ cuando $k \rightarrow +\infty$, entonces $f(n) = g(n)$ para cada n .

DEMOSTRACIÓN. Sea $h(n) = f(n) - g(n)$ y sea $H(s) = F(s) - G(s)$. Entonces $H(s_k) = 0$ para cada k . Para probar que $h(n) = 0$ para todo n , supongamos que $h(n) \neq 0$ para un cierto n y obtendremos una contradicción.

Sea N el menor entero tal que $h(n) \neq 0$. Entonces

$$H(s) = \sum_{n=N}^{\infty} \frac{h(n)}{n^s} = \frac{h(N)}{N^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Luego

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Si hacemos $s = s_k$ tenemos $H(s_k) = 0$ luego

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} h(n)n^{-s_k}.$$

Elegimos k tal que $\sigma_k > c$ en donde $c > \sigma_a$. Entonces el lema 1 implica

$$|h(N)| \leq N^{\sigma_k} (N+1)^{-(\sigma_k-c)} \sum_{n=N+1}^{\infty} |h(n)| n^{-c} = \left(\frac{N}{N+1} \right)^{\sigma_k} A$$

en donde A no depende de k . Si hacemos que $k \rightarrow \infty$ obtenemos $(N/(N+1))^{\sigma_k} \rightarrow 0$ luego $h(N) = 0$, que es una contradicción. $\square$

El teorema de unicidad implica la existencia de un semiplano en el cual la serie de Dirichlet no puede anularse (al menos que se anule idénticamente).

Teorema 11.4 Sea $F(s) = \sum f(n)n^{-s}$ y supongamos que $F(s) \neq 0$ para un cierto s con $\sigma < \sigma_a$. Entonces existe un semiplano $\sigma > c \geq \sigma_a$ en el que $F(s)$ nunca es cero.

DEMOSTRACIÓN. Supongamos que tal semiplano no existe. Entonces, para cada $k = 1, 2, \dots$ existe un punto s_k con $\sigma_k > k$ tal que $F(s_k) = 0$. Dado que $\sigma_k \rightarrow +\infty$ cuando $k \rightarrow \infty$ el teorema de unicidad prueba que $f(n) = 0$ para todo n , en contradicción con la hipótesis de que $F(s) \neq 0$ para un s . $\square$

11.4 MULTIPLICACIÓN DE SERIES DE DIRICHLET

El teorema que sigue relaciona los productos de series de Dirichlet con la convolución de Dirichlet de sus coeficientes.

Teorema 11.5 Dadas dos funciones $F(s)$ y $G(s)$ representadas por dos series de Dirichlet,

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{para } \sigma > a,$$

y

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \text{para } \sigma > b.$$

Entonces, en el semiplano en el que ambas series convergen absolutamente, tenemos

$$(5) \quad F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s},$$

en donde $h = f * g$, es la convolución de Dirichlet de f y g :

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Recíprocamente, si $F(s)G(s) = \sum \alpha(n)n^{-s}$ para todo s de una sucesión $\{s_k\}$ con $\sigma_k \rightarrow +\infty$ cuando $k \rightarrow \infty$, entonces $\alpha = f * g$.

DEMOSTRACIÓN. Para todo s en el que ambas series converjan absolutamente tenemos

$$F(s)G(s) = \sum_{n=1}^{\infty} f(n)n^{-s} \sum_{m=1}^{\infty} g(m)m^{-s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} f(n)g(m)(mn)^{-s}.$$

En virtud de la convergencia absoluta podemos multiplicar estas series y reordenar sus términos convenientemente sin que ello altere la suma. Juntamos los términos para los que mn es constante, $mn = k$. Los posibles valores de k son $1, 2, \dots$, luego

$$F(s)G(s) = \sum_{k=1}^{\infty} \left(\sum_{mn=k} f(n)g(m) \right) k^{-s} = \sum_{k=1}^{\infty} h(k)k^{-s}$$

en donde $h(k) = \sum_{mn=k} f(n)g(m) = (f * g)(k)$. Hemos demostrado la primera afirmación y la segunda se sigue inmediatamente del teorema de unicidad. $\square$

EJEMPLO 1 Las series $\sum n^{-s}$ y $\sum \mu(n)n^{-s}$ convergen absolutamente para $\sigma > 1$. Si hacemos $f(n) = 1$ y $g(n) = \mu(n)$ en (5) obtenemos $h(n) = [1/n]$, luego

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 \quad \text{si } \sigma > 1.$$

En particular, esto prueba que $\zeta(s) \neq 0$ para $\sigma > 1$ y que

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} \quad \text{si } \sigma > 1.$$

EJEMPLO 2 Con más generalidad, suponemos $f(1) \neq 0$, y sea $g = f^{-1}$, la serie de Dirichlet inversa de f . Entonces en todo semiplano en el que ambas series $F(s) = \sum f(n)n^{-s}$ y $G(s) = \sum g(n)n^{-s}$ convergen absolutamente tenemos $F(s) \neq 0$ y $G(s) = 1/F(s)$.

EJEMPLO 3 Suponemos que $F(s) = \sum f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$. Si f es completamente multiplicativa tenemos $f^{-1}(n) = \mu(n)f(n)$. Como $|f^{-1}(n)| \leq f(n)$, la serie $\sum \mu(n)f(n)n^{-s}$ también converge absolutamente para $\sigma > \sigma_a$ y tenemos

$$\sum_{n=1}^{\infty} \frac{\mu(n)f(n)}{n^s} = \frac{1}{F(s)} \quad \text{si } \sigma > \sigma_a.$$

En particular, para cada carácter de Dirichlet χ , tenemos

$$\sum_{n=1}^{\infty} \frac{\mu(n)\chi(n)}{n^s} = \frac{1}{L(s, \chi)} \quad \text{si } \sigma > 1.$$

EJEMPLO 4 Tomamos $f(n) = 1$ y $g(n) = \varphi(n)$, indicatriz de Euler. Como $\varphi(n) \leq n$, la serie $\sum \varphi(n)n^{-s}$ converge absolutamente para $\sigma > 2$. Luego $h(n) = \sum_{d|n} \varphi(d) = n$, y (5) nos proporciona

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1) \quad \text{si } \sigma > 2.$$

Por consiguiente

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \quad \text{si } \sigma > 2.$$

EJEMPLO 5. Hacemos $f(n) = 1$ y $g(n) = n^a$. Entonces $h(n) = \sum_{d|n} d^a = \sigma_a(n)$, y (5) nos proporciona

$$\zeta(s)\zeta(s-a) = \sum_{n=1}^{\infty} \frac{\sigma_a(n)}{n^s} \quad \text{si } \sigma > \max\{1, 1 + \operatorname{Re}(a)\}.$$

EJEMPLO 6 Hacemos $f(n) = 1$ y $g(n) = \lambda(n)$, función de Liouville. Entonces

$$h(n) = \sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n = m^2 \text{ para un } m, \\ 0 & \text{en otro caso,} \end{cases}$$

luego (5) nos proporciona

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \sum_{\substack{n=1 \\ n=\text{cuadrado}}}^{\infty} \frac{1}{n^s} = \sum_{m=1}^{\infty} \frac{1}{m^{2s}} = \zeta(2s).$$

Por lo tanto

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)} \quad \text{si } \sigma > 1.$$

11.5 PRODUCTOS DE EULER

El próximo teorema, descubierto por Euler en 1737, a veces, se denomina versión analítica del teorema fundamental de la Aritmética.

Teorema 11.6 *Sea f una función aritmética multiplicativa tal que la serie $\sum f(n)$ es absolutamente convergente. Entonces la suma de la serie se puede expresar como un producto infinito absolutamente convergente*

$$(6) \quad \sum_{n=1}^{\infty} f(n) = \prod_p \{1 + f(p) + f(p^2) + \cdots\}$$

extendido al conjunto de todos los números primos. Si f es completamente multiplicativa, el producto se simplifica y se tiene

$$(7) \quad \sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1 - f(p)}.$$

Nota. En cada uno de los casos el producto se llama *producto de Euler* de la serie.

DEMOSTRACIÓN. Consideremos el producto finito

$$P(x) = \prod_{p \leq x} \{1 + f(p) + f(p^2) + \cdots\}$$

extendido a todos los números primos $p \leq x$. Como es el producto de un número finito de términos de una serie absolutamente convergente podemos multiplicar la serie y reordenar sus términos arbitrariamente sin que se altere la suma. Un término tipo es de la forma

$$f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_r^{a_r}) = f(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})$$

ya que f es multiplicativa. Por el teorema fundamental de la Aritmética podemos escribir

$$P(x) = \sum_{n \in A} f(n)$$

en donde A consta de todos los n cuya descomposición tiene factores primos $\leq x$. Por consiguiente

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n),$$

en donde B es el conjunto de los n que tienen por lo menos un factor primo $> x$. Por consiguiente

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|.$$

Cuando $x \rightarrow \infty$ la última suma de la derecha tiende a 0 puesto que $\sum |f(n)|$ es convergente. Luego $P(x) \rightarrow \sum f(n)$ cuando $x \rightarrow \infty$.

Ahora bien, un producto infinito de la forma $\prod (1 + a_n)$ converge absolutamente siempre que la serie asociada $\sum a_n$ converge absolutamente. En este caso tenemos

$$\sum_{p \leq x} |f(p) + f(p^2) + \cdots| \leq \sum_{p \leq x} (|f(p)| + |f(p^2)| + \cdots) \leq \sum_{n=2}^{\infty} |f(n)|.$$

Al estar acotadas todas las sumas parciales, la serie de términos positivos

$$\sum_p |f(p) + f(p^2) + \cdots|$$

converge, y este resultado implica la convergencia absoluta del producto (6).

Finalmente, cuando f es completamente multiplicativa tenemos $f(p^n) = f(p)^n$ y cada serie de la derecha de (6) es una serie geométrica convergente cuya suma es $(1 - f(p))^{-1}$. $\square$

Aplicando el teorema 11.6 a las series de Dirichlet absolutamente convergentes obtenemos inmediatamente:

Teorema 11.7 Suponemos que $\sum f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$. Si f es multiplicativa tenemos

$$(8) \quad \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left\{ 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots \right\} \quad \text{si } \sigma > \sigma_a.$$

y si f es completamente multiplicativa tenemos

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}} \quad \text{si } \sigma > \sigma_a.$$

Obsérvese que el término general del producto (8) es la serie de Bell $f_p(x)$ de la función f con $x = p^{-s}$. (Ver sección 2.16.)

EJEMPLOS Hacemos $f(n) = 1$, $\mu(n)$, $\sigma_a(n)$, $\lambda(n)$ y $\chi(n)$, respectivamente, y obtenemos los siguientes productos de Euler:

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} \quad \text{si } \sigma > 1. \\ \frac{1}{\zeta(s)} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) \quad \text{si } \sigma > 1. \\ \frac{\zeta(s-1)}{\zeta(s)} &= \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_p \frac{1 - p^{-s}}{1 - p^{1-s}} \quad \text{si } \sigma > 2. \\ \zeta(s)\zeta(s-\alpha) &= \sum_{n=1}^{\infty} \frac{\sigma_{\alpha}(n)}{n^s} = \prod_p \frac{1}{(1 - p^{-s})(1 - p^{\alpha-s})} \quad \text{si } \sigma < \max \{1, 1 + \operatorname{Re}(\alpha)^*\}, \\ \frac{\zeta(2s)}{\zeta(s)} &= \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \prod_p \frac{1}{1 + p^{-s}} \quad \text{si } \sigma > 1, \\ L(s, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}} \end{aligned}$$

Nota. Si $\chi = \chi_1$, es el carácter principal mod k , entonces $\chi_1(p) = 0$ si $p|k$ y $\chi_1(p) = 1$ si $p \nmid k$, luego el producto de Euler para $L(s, \chi_1)$ se convierte en

$$L(s, \chi_1) = \prod_{p \nmid k} \frac{1}{1 - p^{-s}} = \prod_p \frac{1}{1 - p^{-s}} \cdot \prod_{p|k} (1 - p^{-s}) = \zeta(s) \prod_{p|k} (1 - p^{-s}).$$

Entonces la L -función $L(s, \chi_1)$ es igual a la función zeta $\zeta(s)$ multiplicada por un número finito de factores.

11.6 EL SEMIPLANO DE CONVERGENCIA DE UNA SERIE DE DIRICHLET

Para demostrar la existencia del semiplano de convergencia utilizaremos el lema que sigue.

Lema 2 Sea $s_0 = \sigma_0 + it_0$ y supongamos que la serie de Dirichlet $\sum f(n)n^{-s_0}$ tiene sumas parciales acotadas, o sea

$$\left| \sum_{n \leq x} f(n)n^{-s_0} \right| \leq M$$

para todo $x \geq 1$. Entonces, para cada s con $\sigma > \sigma_0$, tenemos

$$(9) \quad \left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq 2Ma^{\sigma_0-\sigma} \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right).$$

DEMOSTRACIÓN. Sea $a(n) = f(n)n^{-s_0}$ y sea $A(x) = \sum_{n \leq x} a(n)$. Entonces $f(n)n^{-s} = a(n)n^{s_0-s}$ por lo que podemos aplicar el teorema 4.2 (con $f(x) = x^{s_0-s}$) y obtenemos

$$\sum_{a < n \leq b} f(n)n^{-s} = A(b)b^{s_0-s} - A(a)a^{s_0-s} + (s - s_0) \int_a^b A(t)t^{s_0-s-1} dt.$$

Pero, al ser $|A(x)| \leq M$ resulta

$$\begin{aligned} \left| \sum_{a < n \leq b} f(n)n^{-s} \right| &\leq Mb^{\sigma_0-\sigma} + Ma^{\sigma_0-\sigma} + |s - s_0|M \int_a^b t^{\sigma_0-\sigma-1} dt \\ &\leq 2Ma^{\sigma_0-\sigma} + |s - s_0|M \left| \frac{b^{\sigma_0-\sigma} - a^{\sigma_0-\sigma}}{\sigma_0 - \sigma} \right| \\ &\leq 2Ma^{\sigma_0-\sigma} \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right). \quad \square \end{aligned}$$

EJEMPLOS Si las sumas parciales $\sum_{n \leq x} f(n)$ están acotadas, el lema 2 implica que $\sum f(n)n^{-s}$ converge para $\sigma > 0$. En efecto, si hacemos $s_0 = \sigma_0 = 0$ en (9) obtenemos, para $\sigma > 0$,

$$\left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq Ka^{-\sigma}$$

en donde K es independiente de a . Si hacemos que $a \rightarrow +\infty$ vemos que $\sum f(n)n^{-s}$ converge si $\sigma > 0$. En particular este hecho prueba que la serie de Dirichlet

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

converge para $\sigma > 0$ ya que $|\sum_{n \leq x} (-1)^n| \leq 1$. Análogamente, si χ es un carácter de Dirichlet, mod k , no principal, tenemos $|\sum_{n \leq x} \chi(n)| \leq \varphi(k)$, luego

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

converge para $\sigma < 0$. El mismo tipo de razonamiento lleva al siguiente teorema.

Teorema 11.8 *Si la serie $\sum f(n)n^{-s}$ converge para $s = \sigma_0 + it_0$, entonces también converge para todo s con $\sigma > \sigma_0$. Si diverge para $s = \sigma_0 + it_0$, diverge también para todo s con $\sigma < \sigma_0$.*

DEMOSTRACIÓN. La segunda afirmación se sigue de la primera. Para demostrar la primera afirmación, elegimos un s con $\sigma > \sigma_0$. El lema 2 prueba que

$$\left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq K a^{\sigma_0 - \sigma}$$

en donde K no depende de a . Como $a^{\sigma_0 - \sigma} \rightarrow 0$ cuando $a \rightarrow +\infty$, la condición de Cauchy prueba que $\sum f(n)n^{-s}$ converge. $\square$

Teorema 11.9 *Si la serie $\sum f(n)n^{-s}$ no converge para todo s o no diverge para todo s , entonces existe un número real σ_c , llamado la abscisa de convergencia, tal que la serie converge para todo s del semiplano $\sigma < \sigma_c$ y diverge para todo s del semiplano $\sigma > \sigma_c$.*

DEMOSTRACIÓN. Se razona como en la demostración del teorema 11.1, tomando σ_c igual al supremo de todos los σ tales que $\sum f(n)n^{-s}$ diverge. $\square$

Nota. Si la serie converge para todo s definimos $\sigma_c = -\infty$, y si no converge en ningún punto definimos $\sigma_c = +\infty$.

Como la convergencia absoluta implica la convergencia, en cualquier caso tenemos $\sigma_a \geq \sigma_c$. Si $\sigma_a > \sigma_c$ existe un intervalo infinito $\sigma_c < \sigma < \sigma_a$ en el que la serie converge condicionalmente (ver figura 11.1.) El teorema que sigue prueba que la amplitud de dicho intervalo no excede a 1.

Teorema 11.10 *Para toda serie de Dirichlet con σ_c finito tenemos*

$$0 \leq \sigma_a - \sigma_c \leq 1.$$

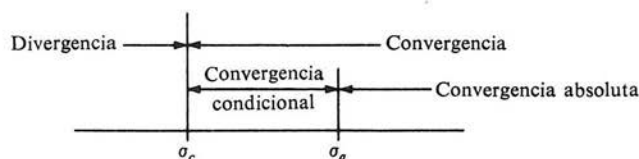


Figura 11.1

DEMOSTRACIÓN. Basta demostrar que, si $\sum f(n)n^{-s_0}$ converge para un cierto s_0 , entonces converge absolutamente para todo s con $\sigma > \sigma_0 + 1$. Sea A una cota superior del conjunto de números $|f(n)n^{-s_0}|$. Entonces

$$\left| \frac{f(n)}{n^s} \right| = \left| \frac{f(n)}{n^{s_0}} \right| \left| \frac{1}{n^{s-s_0}} \right| \leq \frac{A}{n^{\sigma-\sigma_0}}$$

luego $\sum |f(n)n^{-s}|$ converge por comparación con $\sum n^{\sigma_0-\sigma}$. □

EJEMPLO La serie

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

converge si $\sigma > 0$, pero la convergencia únicamente es absoluta si $\sigma > 1$. Por consiguiente en este ejemplo $\sigma_c = 0$ y $\sigma_a = 1$.

Las propiedades de convergencia de las series de Dirichlet se pueden comparar con las propiedades de convergencia de las series de potencias. Cada serie de potencias posee un disco de convergencia, mientras que cada serie de Dirichlet admite un semiplano de convergencia. Para las series de potencias el interior del disco de convergencia es también el dominio de convergencia absoluta. Para las series de Dirichlet el dominio de convergencia absoluta puede constituir un subconjunto propio del dominio de convergencia. Una serie de potencias representa una función analítica en el interior de su disco de convergencia. A continuación demostraremos que una serie de Dirichlet representa una función analítica en el interior del semiplano de convergencia.

11.7 PROPIEDADES ANALÍTICAS DE LAS SERIES DE DIRICHLET

Las propiedades de las series de Dirichlet se deducirán del siguiente teorema general relativo a la teoría de funciones complejas, que damos como lema.

Lema 3 Sea $\{f_n\}$ una sucesión de funciones analíticas en un conjunto abierto S del plano complejo, y supongamos que $\{f_n\}$ converge uniformemente en cada subconjunto compacto de S hacia una función límite f . Entonces f es una función analítica en S y la sucesión de derivadas $\{f'_n\}$ converge uniformemente en cada subconjunto compacto de S hacia la derivada f' .

DEMOSTRACIÓN. Por ser f_n analítica en S tenemos la fórmula integral de Cauchy

$$f_n(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f_n(z)}{z-a} dz$$

en donde D es un disco compacto arbitrario de S , ∂D es su frontera orientada positivamente, y a es un punto interior de D . En virtud de la convergencia uniforme podemos introducir el límite bajo el signo integral y obtener

$$f(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f(z)}{z-a} dz$$

que implica que f es analítica en el interior de D . Para las derivadas tenemos

$$f'_n(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f_n(z)}{(z-a)^2} dz \quad \text{y} \quad f'(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f(z)}{(z-a)^2} dz$$

de donde fácilmente se obtiene que $f'_n(a) \rightarrow f'(a)$ uniformemente en cada subconjunto compacto de S cuando $n \rightarrow \infty$.

Para aplicar el lema a las series de Dirichlet probaremos en primer lugar que tenemos convergencia uniforme en los subconjuntos compactos del semiplano de convergencia.

Teorema 11.11 Una serie de Dirichlet $\sum f(n)n^{-s}$ converge uniformemente en cada subconjunto compacto perteneciente al interior del semiplano de convergencia $\sigma > \sigma_c$.

DEMOSTRACIÓN. Basta probar que $\sum f(n)n^{-s}$ converge uniformemente en cada rectángulo compacto $R = [\alpha, \delta] \times [c, d]$ con $\alpha > \sigma_c$. Para ello utilizamos la acotación obtenida en el lema 2.

$$(10) \quad \left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq 2Ma^{\sigma_0 - \sigma} \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right)$$

en donde $s_0 = \sigma_0 + it$ es un punto arbitrario del semiplano $\sigma > \sigma_c$ y s es un punto arbitrario con $\sigma > \sigma_0$. Elegimos $s_0 = \sigma_0$, en donde $\sigma_c < \sigma_0 < \alpha$. (Ver figura 11.2.)

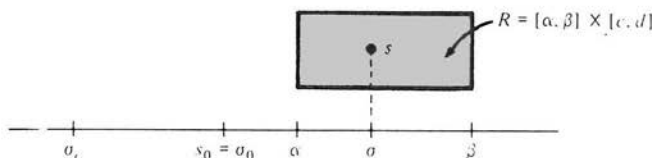


Figura 11.2

Entonces, si $s \in R$, tenemos $\sigma - \sigma_0 \geq \alpha - \sigma_0$ y $|s_0 - s| < C$, en donde C es una constante que depende de s_0 y de R pero, en cambio, no depende de s . Entonces (10) implica

$$\left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq 2Ma^{\sigma_0 - \alpha} \left(1 + \frac{C}{\alpha - \sigma_0} \right) = Ba^{\sigma_0 - \alpha}$$

en donde B es independiente de s . Como $a^{\sigma_0 - \sigma} \rightarrow 0$ cuando $a \rightarrow +\infty$ se verifica la condición de Cauchy de la convergencia uniforme. $\square$

Teorema 11.12 La función suma $F(s) = \sum f(n)n^{-s}$ de una serie de Dirichlet es analítica en su semiplano de convergencia $\sigma > \sigma_c$, y su derivada $F'(s)$ se halla representada en dicho semiplano por la serie de Dirichlet

$$(11) \quad F'(s) = - \sum_{n=1}^{\infty} \frac{f(n) \log n}{n^s},$$

obtenida derivando término a término.

DEMOSTRACIÓN. Aplicamos el teorema 11.11 y el lema 3 a la sucesión de las sumas parciales. $\square$

Notas. La serie derivada (11) tiene la misma abscisa de convergencia y la misma abscisa de convergencia absoluta que la serie relativa a $F(s)$.

Aplicando repetidamente el teorema 11.12, obtenemos que la k -ésima derivada se halla expresada por

$$F^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{f(n)(\log n)^k}{n^s} \quad \text{para } \sigma > \sigma_c.$$

EJEMPLOS Para $\sigma > 1$ tenemos

$$(12) \quad \zeta'(s) = - \sum_{n=1}^{\infty} \frac{\log n}{n^s}$$

y

$$(13) \quad -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

La ecuación (12) se obtiene derivando término a término la serie correspondiente a la función zeta, y (13) se obtiene multiplicando las dos series de Dirichlet $\sum \Lambda(n)n^{-s}$ y $\sum n^{-s}$ y utilizando la identidad $\sum_{d|n} \Lambda(d) = \log n$.

11.8 SERIES DE DIRICHLET CON COEFICIENTES NO NEGATIVOS

Algunas funciones definidas por medio de series de Dirichlet en su semiplano de convergencia $\sigma > \sigma_c$ se pueden prolongar analíticamente más allá de la recta $\sigma = \sigma_c$. Por ejemplo, en el capítulo que sigue demostraremos que la función zeta de Riemann $\zeta(s)$ se puede prolongar analíticamente al otro lado de la recta $\sigma = 1$ a una función que es analítica para todo s salvo en un polo simple, en $s = 1$. Análogamente, si χ es un carácter de Dirichlet no principal, la L -función $L(s, \chi)$ se puede prolongar analíticamente al otro lado de la recta $\sigma = 1$ a una función entera (analítica para todo s). La singularidad de la función zeta se explica por el teorema de Landau que sigue referente a series de Dirichlet con coeficientes no negativos.

Teorema 11.13 Sea $F(s)$ representada en el semiplano $\sigma > c$ por la serie de Dirichlet

$$(14) \quad F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

en donde c es finito, y supongamos que $f(n) \geq 0$ para todo $n \geq n_0$. Si $F(s)$ es analítica en un disco que contiene en su interior el punto $s = c$, entonces la serie de Dirichlet converge en el semiplano $\sigma > c - \varepsilon$ para un $\varepsilon > 0$. En consecuencia, si la serie de Dirichlet posee abscisa de convergencia finita σ_c , entonces $F(s)$ posee una singularidad en el eje real en el punto $s = \sigma_c$.

DEMOSTRACIÓN. Sea $a = 1 + c$. Dado que F es analítica en a , se puede representar por medio de un desarrollo en serie de potencias centrado en a , absolutamente convergente,

$$(15) \quad F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!} (s-a)^k,$$

y el radio de convergencia de esta serie de potencias excede a 1 puesto que F es analítica en c . (Ver figura 11.3.) Por el teorema 11.12, es posible mediante derivación sucesiva de (14) determinar la derivada $F^{(k)}(a)$. Esto nos proporciona

$$F^{(k)}(a) = (-1)^k \sum_{n=1}^{\infty} f(n) (\log n)^k n^{-a},$$

luego (15) se puede escribir en la forma

$$(16) \quad F(s) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(a-s)^k}{k!} f(n) (\log n)^k n^{-a}.$$

Como el radio de convergencia excede de 1, esta fórmula es válida para un real $s = c - \varepsilon$ en donde $\varepsilon > 0$ (ver figura 11.3). Entonces $a - s = 1 + \varepsilon$ para este s y la serie doble (16) tiene sus términos no negativos para $n \geq n_0$. Por consiguiente podemos cambiar el orden de los sumandos para obtener

$$F(c - \varepsilon) = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{\{(1 + \varepsilon) \log n\}^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(1 + \varepsilon) \log n} = \sum_{n=1}^{\infty} \frac{f(n)}{n^{c - \varepsilon}}.$$

Con otras palabras, la serie de Dirichlet $\sum f(n)n^{-s}$ converge para $s = c - \varepsilon$, luego también converge en el semiplano $\sigma > c - \varepsilon$. $\square$

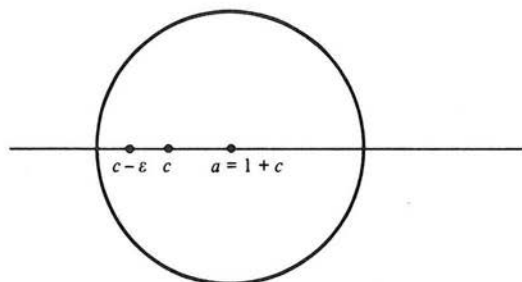


Figura 11.3

11.9 SERIES DE DIRICHLET EXPRESADAS COMO EXPONENCIALES DE SERIES DE DIRICHLET

Una serie de Dirichlet $F(s) = \sum f(n)n^{-s}$ que no se anula idénticamente admite un semiplano en el que no se anula. El teorema que sigue demuestra que en este semiplano $F(s)$ es la exponencial de otra serie de Dirichlet si $f(1) \neq 0$.

Teorema 11.14 Sea $F(s) = \sum f(n)n^{-s}$ absolutamente convergente para $\sigma > \sigma_0$ y supongamos que $f(1) \neq 0$. Si $F(s) \neq 0$ para $\sigma > \sigma_0 \geq \sigma_a$, entonces para $\sigma > \sigma_0$ tenemos

$$F(s) = e^{G(s)}$$

con

$$G(s) = \log f(1) + \sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{\log n} n^{-s},$$

en donde f^{-1} es la inversa de Dirichlet de f y $f'(n) = f(n) \log n$.

Nota. Para z complejo $\neq 0$, $\log z$ designa la rama del logaritmo que es real cuando $z > 0$.

DEMOSTRACIÓN. Como $F(s) \neq 0$, podemos escribir $F(s) = e^{G(s)}$, donde $G(s)$ es una función analítica para $\sigma > \sigma_0$. Diferenciando obtenemos

$$F'(s) = e^{G(s)} G'(s) = F(s) G'(s),$$

luego $G'(s) = F'(s)/F(s)$. Pero

$$F'(s) = - \sum_{n=1}^{\infty} \frac{f(n) \log n}{n^s} = - \sum_{n=1}^{\infty} \frac{f'(n)}{n^s} \quad \text{y} \quad \frac{1}{F(s)} = \sum_{n=1}^{\infty} \frac{f^{-1}(n)}{n^s},$$

por lo tanto

$$G'(s) = F'(s) \cdot \frac{1}{F(s)} = - \sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{n^s}.$$

Integrando obtenemos

$$G(s) = C + \sum_{n=2}^{\infty} \frac{(f' * f^{-1})(n)}{\log n} n^{-s}$$

en donde C es una constante. Si hacemos que $\sigma \rightarrow +\infty$ vemos que $\lim_{\sigma \rightarrow \infty} G(\sigma + it) = C$, luego

$$f(1) = \lim_{\sigma \rightarrow \infty} F(\sigma + it) = e^C$$

o sea $C = \log f(1)$. Este resultado termina la demostración. Esta demostración prueba también que la serie relativa a $G(s)$ converge absolutamente si $\sigma > \sigma_0$. $\square$

EJEMPLO 1 Cuando $f(n) = 1$ tenemos $f'(n) = \log n$ y $f^{-1}(n) = \mu(n)$ o sea

$$(f' * f^{-1})(n) = \sum_{d|n} \log d \mu\left(\frac{n}{d}\right) = \Lambda(n).$$

Por consiguiente, si $\sigma > 1$, tenemos

$$(17) \quad \zeta(s) = e^{G(s)}$$

en donde

$$G(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}.$$

EJEMPLO 2 Un razonamiento análogo prueba que si f es completamente multiplicativa y $F(s) = \sum f(n)n^{-s}$ entonces, en el semiplano de convergencia absoluta $\sigma > \sigma_a$ tenemos

$$F(s) = e^{G(s)}$$

en donde

$$G(s) = \sum_{n=2}^{\infty} \frac{f(n)\Lambda(n)}{\log n} n^{-s}$$

puesto que $(f' * f)(n) = \sum_{d|n} f(d) \log d \mu(n/d) f(n/d) = f(n)\Lambda(n)$.

Las fórmulas de los ejemplos anteriores se pueden deducir también mediante los productos de Euler. Por ejemplo, en lo que se refiere a la función zeta de Riemann tenemos

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Mantenemos s real, $s > 1$, por lo que $\zeta(s)$ es positiva. Si ahora tomamos logaritmos y utilizamos la serie de potencias $-\log(1-x) = \sum x^m/m$ obtenemos

$$\log \zeta(s) = - \sum_p \log(1 - p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} \Lambda_1(n) n^{-s}$$

en donde

$$\Lambda_1(n) = \begin{cases} \frac{1}{m} & \text{si } n = p^m \text{ para un primo } p, \\ 0 & \text{en otro caso.} \end{cases}$$

Pero si $n = p^m$ entonces $\log n = m \log p = m \Lambda(n)$ por lo que $1/m = \Lambda(n)/\log n$. Por consiguiente

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}$$

que implica (17) para s real > 1 . Pero cada miembro de (17) es analítico en el semiplano $\sigma > 1$ luego, por prolongación analítica, (17) también se verifica para $\sigma > 1$.

11.10 FÓRMULAS DE VALOR MEDIO PARA SERIES DE DIRICHLET

Teorema 11.15 *Se dan dos series de Dirichlet $F(s) = \sum f(n)n^{-s}$ y $G(s) = \sum g(n)n^{-s}$ con abscisas de convergencia absoluta σ_1 y σ_2 , respectivamente. Entonces para $a > \sigma_1$ y $b > \sigma_2$ tenemos*

$$\lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T F(a + it) G(b - it) dt = \sum_{n=1}^{\infty} \frac{f(n)g(n)}{n^{a+b}}.$$

DEMOSTRACIÓN. Tenemos

$$\begin{aligned} F(a + it) G(b - it) &= \left(\sum_{m=1}^{\infty} \frac{f(m)}{m^{a+it}} \right) \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^{b-it}} \right) = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)g(n)}{m^a n^b} \left(\frac{n}{m} \right)^{it} \\ &= \sum_{n=1}^{\infty} \frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m=1 \\ m \neq n}}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)g(n)}{m^a n^b} \left(\frac{n}{m} \right)^{it}. \end{aligned}$$

Ahora bien

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \left| \frac{f(m)g(n)}{m^a n^b} \left(\frac{n}{m} \right)^{it} \right| \leq \sum_{m=1}^{\infty} \frac{|f(m)|}{m^a} \sum_{n=1}^{\infty} \frac{|g(n)|}{n^b}$$

luego la serie es absolutamente convergente, y esta convergencia es también uni-

forme para todo t . Por lo tanto podemos integrar término a término y dividir por $2T$ para obtener

$$\begin{aligned} \frac{1}{2T} \int_{-T}^T F(a+it)G(b-it) dt \\ = \sum_{n=1}^{\infty} \frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m, n=1 \\ m \neq n}}^{\infty} \frac{f(m)g(n)}{m^a n^b} \frac{1}{2T} \int_{-T}^T e^{it \log(n/m)} dt. \end{aligned}$$

Pero, para $m \neq n$, tenemos

$$\int_{-T}^T e^{it \log(n/m)} dt = \frac{e^{it \log(n/m)}}{i \log(n/m)} \Big|_{-T}^T = \frac{2 \operatorname{sen} \left[T \log \left(\frac{n}{m} \right) \right]}{\log \left(\frac{n}{m} \right)}$$

por lo que obtenemos

$$\begin{aligned} \frac{1}{2T} \int_{-T}^T F(a+it)G(b-it) dt \\ = \sum_{n=1}^{\infty} \frac{f(n)g(n)}{n^{a+b}} + \sum_{\substack{m, n=1 \\ m \neq n}}^{\infty} \frac{f(m)g(n)}{m^a n^b} \frac{\operatorname{sen} \left[T \log \left(\frac{n}{m} \right) \right]}{T \log \left(\frac{n}{m} \right)}. \end{aligned}$$

De nuevo, la serie doble converge uniformemente respecto a T ya que $(\operatorname{sen} x)/x$ está acotado para cada x . Luego, si en cada término tomamos límites obtenemos la afirmación del teorema. $\square$

Teorema 11.16 Si $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$, entonces para $\sigma > \sigma_a$ tenemos

$$(18) \quad \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |F(\sigma + it)|^2 dt = \sum_{n=1}^{\infty} \frac{|f(n)|^2}{n^{2\sigma}}.$$

En particular, si $\sigma > 1$ tenemos

$$(a) \quad \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |\zeta(\sigma + it)|^2 dt = \sum_{n=1}^{\infty} \frac{1}{n^{2\sigma}} = \zeta(2\sigma).$$

$$(b) \quad \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |\zeta^{(k)}(\sigma + it)|^2 dt = \sum_{n=1}^{\infty} \frac{\log^{2k} n}{n^{2\sigma}} = \zeta^{(2k)}(2\sigma).$$

$$(c) \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |\zeta(\sigma + it)|^{-2} dt = \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^{2\sigma}} = \frac{\zeta(2\sigma)}{\zeta(4\sigma)}.$$

$$(d) \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T |\zeta(\sigma + it)|^4 dt = \sum_{n=1}^{\infty} \frac{\sigma_0^2(n)}{n^{2\sigma}} = \frac{\zeta^4(2\sigma)}{\zeta(4\sigma)}.$$

DEMOSTRACIÓN. Si en el teorema 11.15 hacemos $g(n) = \overline{f(n)}$ obtenemos la fórmula (18). Para deducir las fórmulas especiales (a), (b), (c) y (d) debemos calcular tan sólo el valor de las series de Dirichlet $\sum |f(n)|^2 n^{-2\sigma}$ para las siguientes elecciones de $f(n)$: (a) $f(n) = 1$; (b) $f(n) = (-1)^k \log^k n$; (c) $f(n) = \mu(n)$; (d) $f(n) = \sigma_0(n)$. La fórmula (a) es clara, y la fórmula (b) se sigue de la relación

$$\zeta^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{\log^k n}{n^s}.$$

Para probar (c) y (d) utilizamos productos de Euler. Para (c) tenemos

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \prod_p (1 + p^{-s}) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(2s)}.$$

Si sustituimos s por 2σ obtenemos (c). Para llegar a (d) escribimos

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\sigma_0^2(n)}{n^s} &= \prod_p \{1 + \sigma_0^2(p)p^{-s} + \sigma_0^2(p^2)p^{-2s} + \dots\} \\ &= \prod_p \{1 + 2^2 p^{-s} + 3^2 p^{-2s} + \dots\} \\ &= \prod_p \left\{ \sum_{n=0}^{\infty} (n+1)^2 p^{-ns} \right\} = \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})^4} = \frac{\zeta^4(s)}{\zeta(2s)} \end{aligned}$$

ya que $\sum_{n=0}^{\infty} (n+1)^2 x^n = \frac{x+1}{(x-1)^3} = \frac{1-x^2}{(1-x)^4}$. Ahora sustituimos s por 2σ y obtenemos (d). $\square$

11.11 UNA FÓRMULA INTEGRAL PARA LOS COEFICIENTES DE UNA SERIE DE DIRICHLET

Teorema 11.17 Suponemos que la serie $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ es absolutamente convergente para $\sigma > \sigma_a$. Entonces, para $\sigma > \sigma_a$ y $x > 0$, tenemos

$$\lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T F(\sigma + it) x^{\sigma+it} dt = \begin{cases} f(n) & \text{si } x = n, \\ 0 & \text{en otro caso.} \end{cases}$$

DEMOSTRACIÓN. Para $\sigma > \sigma_a$ tenemos

$$\begin{aligned} (19) \quad \frac{1}{2T} \int_{-T}^T F(\sigma + it) x^{\sigma+it} dt &= \frac{x^\sigma}{2T} \int_{-T}^T \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} \left(\frac{x}{n}\right)^{it} dt \\ &= \frac{x^\sigma}{2T} \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} \int_{-T}^T e^{it \log(x/n)} dt, \end{aligned}$$

ya que la serie es uniformemente convergente para todo t del intervalo $[-T, T]$. Si x no es entero, entonces $x/n \neq 1$ para todo n y tenemos

$$\int_{-T}^T e^{it \log(x/n)} dt = \frac{2 \operatorname{sen} \left[T \log \left(\frac{x}{n} \right) \right]}{\log \left(\frac{x}{n} \right)}$$

y la serie se transforma en

$$\frac{x^\sigma}{T} \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} \frac{\operatorname{sen} \left[T \log \left(\frac{x}{n} \right) \right]}{\log \left(\frac{x}{n} \right)}$$

que tiende a 0 cuando $T \rightarrow \infty$. Sin embargo, si x es un entero, por ejemplo $x = k$, entonces el término (19), para $n = k$, contribuye con

$$\int_{-T}^T \left(\frac{x}{n}\right)^{it} dt = \int_{-T}^T \left(\frac{k}{k}\right)^{it} dt = \int_{-T}^T 1 dt = 2T,$$

y por consiguiente

$$\frac{x^\sigma}{2T} \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} \int_{-T}^T \left(\frac{x}{n}\right)^{it} dt = f(k) + \frac{k^\sigma}{2T} \sum_{\substack{n=1 \\ n \neq k}}^{\infty} \frac{f(n)}{n^\sigma} \int_{-T}^T \left(\frac{k}{n}\right)^{it} dt.$$

El segundo término tiende a 0 cuando $T \rightarrow \infty$ como veíamos en la primera parte de la demostración. $\square$

11.12 UNA FÓRMULA INTEGRAL PARA LAS SUMAS PARCIALES DE UNA SERIE DE DIRICHLET

En esta sección obtenemos una fórmula de Perron que expresa las sumas parciales de una serie de Dirichlet como integral de la función suma. Precisamos de un lema relativo a las integrales de contorno.

Lema 4 Si $c > 0$, definimos $\int_{c-\infty i}^{c+\infty i}$ como $\lim_{T \rightarrow \infty} \int_{c-iT}^{c+iT}$. Entonces, si a es un número real positivo, tenemos

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} a^z \frac{dz}{z} = \begin{cases} 1 & \text{si } a > 1, \\ \frac{1}{2} & \text{si } a = 1, \\ 0 & \text{si } 0 < a < 1. \end{cases}$$

Además, tenemos

$$(20) \quad \left| \frac{1}{2\pi i} \int_{c-iT}^{c+iT} a^z \frac{dz}{z} \right| \leq \frac{a^c}{\pi T \log\left(\frac{1}{a}\right)} \quad \text{si } 0 < a < 1,$$

$$(21) \quad \left| \frac{1}{2\pi i} \int_{c-iT}^{c+iT} a^z \frac{dz}{z} - 1 \right| \leq \frac{a^c}{\pi T \log a} \quad \text{si } a > 1,$$

y

$$(22) \quad \left| \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{dz}{z} - \frac{1}{2} \right| \leq \frac{c}{\pi T} \quad \text{si } a = 1.$$

DEMOSTRACIÓN. En primer lugar suponemos que $0 < a < 1$ y consideramos el rectángulo de contorno R dado en la figura 11.4. Como a^z/z es analítica en el interior de R tenemos $\int_R a^z/z dz = 0$. Luego

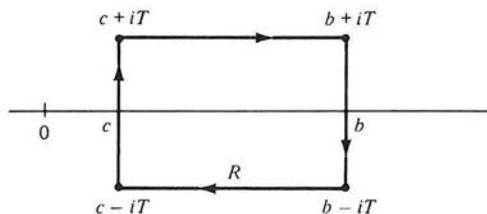


Figura 11.4

$$\int_{c-iT}^{c+iT} = \int_{b+iT}^{c+iT} + \int_{b-iT}^{b+iT} + \int_{c-iT}^{b-iT},$$

por lo tanto

$$\begin{aligned} \left| \int_{c-iT}^{c+iT} a^z \frac{dz}{z} \right| &\leq \int_c^b \frac{a^x}{T} dx + \frac{2Ta^b}{b} + \int_c^b \frac{a^x}{T} dx \\ &\leq \frac{2}{T} \int_c^\infty a^x dx + \frac{2Ta^b}{b} = \frac{2}{T} \left(\frac{-a^c}{\log a} \right) + \frac{2Ta^b}{b}. \end{aligned}$$

Si $b \rightarrow \infty$, obtenemos que $a^b \rightarrow 0$, luego

$$\left| \int_{c-iT}^{c+iT} a^z \frac{dz}{z} \right| \leq \frac{2a^c}{T \log\left(\frac{1}{a}\right)}.$$

Esto termina la demostración de (20).

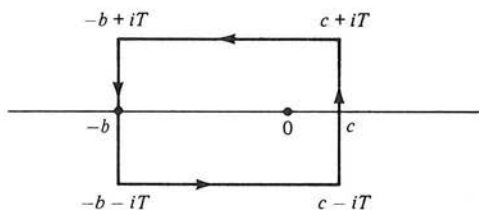


Figura 11.5

Si $a > 1$, utilizamos como contorno R el dibujado en la figura 11.5, en vez del anterior. Aquí $b > c > 0$ y $T > c$. Ahora a^z/z tiene un polo de primer orden en $z = 0$ con residuo 1 puesto que

$$a^z = e^{z \log a} = 1 + z \log a + O(|z|^2) \text{ cuando } z \rightarrow 0.$$

Por consiguiente

$$2\pi i = \left(\int_{c-iT}^{c+iT} + \int_{c+iT}^{-b+iT} + \int_{-b+iT}^{-b-iT} + \int_{-b-iT}^{c-iT} \right) a^z \frac{dz}{z},$$

luego

$$\frac{1}{2\pi i} \int_{c-iT}^{c+iT} a^z \frac{dz}{z} - 1 = \frac{1}{2\pi i} \left(\int_{-b+iT}^{c+iT} + \int_{-b-iT}^{c-iT} + \int_{c-iT}^{-b-iT} \right) a^z \frac{dz}{z}.$$

Ahora calculamos las integrales de la derecha. Obtenemos

$$\begin{aligned} \left| \int_{-b+iT}^{c+iT} a^z \frac{dz}{z} \right| &\leq \int_{-b}^c \frac{a^x dx}{T} \leq \frac{1}{T} \int_{-\infty}^c a^x dx = \frac{1}{T} \frac{a^c}{\log a}, \\ \left| \int_{-b-iT}^{-b+iT} a^z \frac{dz}{z} \right| &\leq 2T \frac{a^{-b}}{b}, \\ \left| \int_{c-iT}^{-b-iT} a^z \frac{dz}{z} \right| &\leq \int_{-b}^c \frac{a^x dx}{T} \leq \frac{1}{T} \frac{a^c}{\log a}. \end{aligned}$$

Y cuando $b \rightarrow \infty$ la segunda integral tiende a 0 y se obtiene (21).

Cuando $a = 1$, la integral se puede tratar directamente. Tenemos

$$\begin{aligned} \int_{c-iT}^{c+iT} \frac{dz}{z} &= \int_{-T}^T \frac{i dy}{c + iy} = \int_{-T}^T \frac{y}{c^2 + y^2} dy + ic \int_{-T}^T \frac{dy}{c^2 + y^2} \\ &= 2ic \int_0^T \frac{dy}{c^2 + y^2}, \end{aligned}$$

ya que al ser la función que se integra una función impar la otra integral se anula. Por lo tanto

$$\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{dz}{z} = \frac{c}{\pi} \int_0^T \frac{dy}{c^2 + y^2} = \frac{1}{\pi} \arctan \frac{T}{c} = \frac{1}{2} - \frac{1}{\pi} \arctan \frac{c}{T}.$$

El hecho de que $\arctan c/T < c/T$ prueba (22), y la demostración del lema 4 queda establecida. $\square$

Teorema 11.18 Fórmula de Perron. Sea $F(s) = \sum_{n=1}^{\infty} f(n)/n^s$ absolutamente convergente para $\sigma > \sigma_a$; sean $c > 0$, $x > 0$ arbitrario. Entonces, si $\sigma > \sigma_a - c$, tenemos:

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} F(s+z) \frac{x^z}{z} dz = \sum_{n \leq x}^* \frac{f(n)}{n^s}$$

en donde $\sum^*$ significa que si x es entero, el último término de la suma se multiplicará por $1/2$.

DEMOSTRACIÓN. En la integral, c es la parte real de z , luego la serie relativa a $F(s+z)$ es absoluta y uniformemente convergente sobre conjuntos compactos del semiplano $\sigma + c > \sigma_a$. Por consiguiente

$$\begin{aligned}
\int_{c-iT}^{c+iT} F(s+z) \frac{x^z}{z} dz &= \int_{c-iT}^{c+iT} \sum_{n=1}^{\infty} \frac{f(n)}{n^{s+z}} \frac{x^z}{z} dz \\
&= \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^z \frac{dz}{z} \\
&= \sum_{n < x} \frac{f(n)}{n^s} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^z \frac{dz}{z} + \sum_{n > x} \frac{f(n)}{n^s} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^z \frac{dz}{z} \\
&\quad + \frac{f(x)}{x^s} \int_{c-iT}^{c+iT} \frac{dz}{z},
\end{aligned}$$

en donde el símbolo $+$ ' indica que el último término interviene sólo cuando x es un entero. En la suma finita $\sum_{n < x}$ podemos pasar al límite, término a término, haciendo que $T \rightarrow \infty$, y la integral es $2\pi i$ por el lema 4. (Aquí $a = x/n$, $a > 1$.) El último término (si aparece) produce $\pi i f(x) x^{-s}$ y el teorema quedará definitivamente establecido en cuanto demosremos que

$$(23) \quad \lim_{T \rightarrow \infty} \sum_{n > x} \frac{f(n)}{n^s} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^z \frac{dz}{z} = 0.$$

Sabemos que $\int_{c-i\infty}^{c+i\infty} (x/n)^z (dz/z) = 0$ si $n > x$, pero para probar (23) es preciso estimar cómo tiende a cero $\int_{c-iT}^{c+iT}$.

Del lema 4 obtenemos la acotación

$$\left| \int_{c-iT}^{c+iT} a^z \frac{dz}{z} \right| \leq \frac{2}{T} \frac{a^c}{\left(\log \frac{1}{a}\right)} \quad \text{si } 0 < a < 1.$$

Aquí $a = x/n$, con $n < x$. En efecto, $n \geq [x] + 1$, o sea que $1/a = n/x \geq ([x] + 1)/x$. Luego

$$\begin{aligned}
\left| \sum_{n > x} \frac{f(n)}{n^s} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^z \frac{dz}{z} \right| &\leq \sum_{n > x} \frac{|f(n)|}{n^{\sigma}} \frac{2}{T} \left(\frac{x}{n}\right)^c \frac{1}{\log \left(\frac{[x] + 1}{x}\right)} \\
&= \frac{2}{T} \frac{x^c}{\log \left(\frac{[x] + 1}{x}\right)} \sum_{n > x} \frac{|f(n)|}{n^{\sigma+c}} \rightarrow 0 \quad \text{cuando } T \rightarrow \infty.
\end{aligned}$$

Hemos demostrado, pues, la fórmula de Perron. □

Nota. Si $c > \sigma_a$ la fórmula de Perron es válida para $s = 0$ y obtenemos la siguiente representación integral de las sumas parciales de los coeficientes:

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} F(z) \frac{x^z}{z} dz = \sum_{n \leq x}^* f(n).$$

Ejercicios del capítulo 11

1. Obtener las siguientes identidades, válidas para $\sigma > 1$,

(a) $\zeta(s) = s \int_1^\infty \frac{[x]}{x^{s+1}} dx$, en donde la suma se halla extendida a todos los primos.

(b) $\sum_p \frac{1}{p^s} = s \int_1^\infty \frac{\pi(x)}{x^{s+1}} dx$,

(c) $\frac{1}{\zeta(s)} = s \int_1^\infty \frac{M(x)}{x^{s+1}} dx$, en donde $M(x) = \sum_{n \leq x} \mu(n)$.

(d) $-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(x)}{x^{s+1}} dx$, en donde $\psi(x) = \sum_{n \leq x} \Lambda(n)$.

(e) $L(s, \chi) = s \int_1^\infty \frac{A(x)}{x^{s+1}} dx$, en donde $A(x) = \sum_{n \leq x} \chi(n)$.

Probar que (e) vale también para $\sigma > 0$ si χ es un carácter no principal. [Indicación: Teorema 4.2.]

2. Suponemos que la serie $\sum_{n=1}^\infty f(n)$ converge y tiene suma A , y definimos $A(x) = \sum_{n \leq x} f(n)$.

(a) Probar que la serie de Dirichlet $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ converge para cada s con $\sigma > 0$ y que

$$\sum_{n=1}^\infty \frac{f(n)}{n^s} = A - s \int_1^\infty \frac{R(x)}{x^{s+1}} dx,$$

en donde $R(x) = A - A(x)$. [Indicación: teorema 4.2.]

(b) Deducir que $F(\sigma) \rightarrow A$ cuando $\sigma \rightarrow 0+$.

(c) Si $\sigma > 0$ y $N \geq 1$ es un entero, probar que

$$F(s) = \sum_{n=1}^N \frac{f(n)}{n^s} - \frac{A(N)}{N^s} + s \int_N^\infty \frac{A(y)}{y^{s+1}} dy.$$

(d) Escribir $s = \sigma + it$, tomar $N = 1 + [t]$ en la parte (c) y probar que

$$|F(\sigma + it)| = O(|t|^{1-\sigma}) \quad \text{si } 0 < \sigma < 1.$$

3. (a) Probar que la serie $\sum_n^{-1-it}$ posee sumas parciales acotadas si $t \neq 0$. Cuando $t = 0$ las sumas parciales no están acotadas.

- (b) Probar que la serie $\sum n^{-1-it}$ diverge para todo real t . Con otras palabras, la serie de Dirichlet relativa a $\zeta(s)$ diverge en toda la recta $\sigma = 1$.
4. Sea $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$, en donde $f(n)$ es completamente multiplicativa y la serie converge absolutamente para $\sigma > \sigma_a$. Probar que, si $\sigma > \sigma_a$, tenemos

$$\frac{F'(s)}{F(s)} = - \sum_{n=1}^{\infty} \frac{f(n)\Lambda(n)}{n^s}.$$

En los ejercicios siguientes, $\lambda(n)$ es la función de Liouville, $d(n)$ es el número de divisores de n , $\nu(n)$ y $\kappa(n)$ están definidas como sigue: $\nu(1) = 0$, $\kappa(1) = 1$; si $n = p_1^{a_1} \dots p_k^{a_k}$, entonces $\nu(n) = k$ y $\kappa(n) = a_1 a_2 \dots a_k$. Probar que las identidades de los ejercicios 5 al 10 son válidos para $\sigma > 1$.

$$\begin{array}{ll} 5. \sum_{n=1}^{\infty} \frac{d(n^2)}{n^s} = \frac{\zeta^3(s)}{\zeta(2s)}. & 8. \sum_{n=1}^{\infty} \frac{2^{\nu(n)}\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta^2(s)}. \\ 6. \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = \zeta(s) \sum_p \frac{1}{p^s}. & 9. \sum_{n=1}^{\infty} \frac{\kappa(n)}{n^s} = \frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}. \\ 7. \sum_{n=1}^{\infty} \frac{2^{\nu(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}. & 10. \sum_{n=1}^{\infty} \frac{3^{\nu(n)}\kappa(n)}{n^s} = \frac{\zeta^3(s)}{\zeta(3s)}. \end{array}$$

11. Expresar la suma de la serie $\sum_{n=1}^{\infty} 3^{\nu(n)}\kappa(n)\lambda(n)n^{-s}$ en términos de la función zeta de Riemann.
12. Sea f una función completamente multiplicativa tal que $f(p) = f(p)^2$ para cada primo p . Si la serie $\sum f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$ y tiene suma $F(s)$, probar que $F(s) \neq 0$ y que

$$\sum_{n=1}^{\infty} \frac{f(n)\lambda(n)}{n^s} = \frac{F(2s)}{F(s)} \quad \text{si } \sigma > \sigma_a.$$

13. Sea f una función multiplicativa tal que $f(p) = f(p)^2$ para cada primo p . Si la serie $\sum \mu(n)f(n)n^{-s}$ converge absolutamente para $\sigma > \sigma_a$ y tiene suma $F(s)$, probar que $F(s) \neq 0$ y que

$$\sum_{n=1}^{\infty} \frac{f(n)|\mu(n)|}{n^s} = \frac{F(2s)}{F(s)} \quad \text{si } \sigma > \sigma_a.$$

14. Sea f una función multiplicativa tal que $\sum f(n)n^{-s}$ converja absolutamente para $\sigma > \sigma_a$. Si p es primo y $\sigma > \sigma_a$ probar que

$$(1 + f(p)p^{-s}) \sum_{n=1}^{\infty} \frac{f(n)\mu(n)}{n^s} = (1 - f(p)p^{-s}) \sum_{n=1}^{\infty} \frac{f(n)\mu(n)\mu(p, n)}{n^s},$$

en donde $\mu(p, n)$ es la función de Möbius evaluada en el mcd de p y n . [Indicación: Productos de Euler.]

15. Probar que

$$\sum_{m=1}^{\infty} \sum_{\substack{n=1 \\ (m,n)=1}}^{\infty} \frac{1}{m^2 n^2} = \frac{\zeta^2(2)}{\zeta(4)}.$$

En general, si cada s_i tiene parte real $\sigma_i > 1$, expresar la suma múltiple

$$\sum_{m_1=1}^{\infty} \cdots \sum_{\substack{m_r=1 \\ (m_1, \dots, m_r)=1}}^{\infty} m_1^{-s_1} \cdots m_r^{-s_r}$$

en términos de la función zeta de Riemann.

16. Las integrales de la forma

$$(24) \quad f(s) = \int_1^{\infty} \frac{A(x)}{x^s} dx,$$

en donde $A(x)$ es integrable Riemann en cada intervalo compacto $[1, a]$, tienen algunas propiedades semejantes a las de las series de Dirichlet. Por ejemplo, poseen un semiplano de convergencia absoluta $\sigma > \sigma_a$ y un semiplano de convergencia $\sigma > \sigma_c$ en el que $f(s)$ es analítica. Este ejercicio describe una proposición análoga a la del teorema 11.13 (*Teorema de Landau*)

Sea $f(s)$ la función representada en el semiplano $\sigma > \sigma_c$ por (24), en donde σ_c es finito, y supongamos que $A(x)$ es una función que toma valores reales y que no cambia de signo para $x \geq x_0$. Probar que $f(s)$ tiene una singularidad sobre el eje real en el punto $s = \sigma_c$.

17. Sea $\lambda_a(n) = \sum_{d|n} d^a \lambda(d)$, en donde $\lambda(n)$ es la función de Liouville. Probar que, si $\sigma > \max\{1, \operatorname{Re}(a) + 1\}$, tenemos

$$\sum_{n=1}^{\infty} \frac{\lambda_a(n)}{n^s} = \frac{\zeta(s)\zeta(2s-2a)}{\zeta(s-a)}$$

y

$$\sum_{n=1}^{\infty} \frac{\lambda(n)\lambda_a(n)}{n^s} = \frac{\zeta(2s)\zeta(s-a)}{\zeta(s)}.$$

Capítulo 12

Las funciones $\zeta(s)$ y $L(s, \chi)$

12.1 INTRODUCCIÓN

Este capítulo desarrolla otras propiedades de la función zeta de Riemann $\zeta(s)$ y de las L -funciones de Dirichlet $L(s, \chi)$ definidas para $\sigma > 1$ por las series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{y} \quad L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Como en el capítulo anterior escribimos $s = \sigma + it$. Es posible unificar el tratamiento de ambas funciones $\zeta(s)$ y $L(s, \chi)$ introduciendo la función zeta de Hurwitz $\zeta(s, a)$, definida para $\sigma > 1$ por la serie

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}.$$

Aquí a es un número real fijo, $0 < a \leq 1$. Cuando $a = 1$ obtenemos la función zeta de Riemann, $\zeta(s) = \zeta(s, 1)$. También es posible expresar $L(s, \chi)$ por medio de la función zeta de Hurwitz. Si χ es un carácter mod k reordenamos los términos de la serie correspondiente a $L(s, \chi)$ de acuerdo con las clases de restos mod k . Esto es, escribimos

$$n = qk + r, \quad \text{en donde } 1 \leq r \leq k \text{ y } q = 0, 1, 2, \dots,$$

y obtenemos

$$\begin{aligned} L(s, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{r=1}^k \sum_{q=0}^{\infty} \frac{\chi(qk+r)}{(qk+r)^s} = \frac{1}{k^s} \sum_{r=1}^k \chi(r) \sum_{q=0}^{\infty} \frac{1}{\left(q + \frac{r}{k}\right)^s} \\ &= k^{-s} \sum_{r=1}^k \chi(r) \zeta\left(s, \frac{r}{k}\right). \end{aligned}$$

Esta representación de $L(s, \chi)$ como combinación lineal de funciones zeta de Hurwitz demuestra que en última instancia las propiedades de las L -funciones dependen de las propiedades de $\zeta(s, a)$.

Nuestro propósito consiste en obtener la prolongación analítica de $\zeta(s, a)$ al otro lado de la recta $\sigma = 1$, lo cual se hace a través de una representación integral de $\zeta(s, a)$ que se obtiene de la fórmula integral correspondiente a la función gamma $\Gamma(s)$.

12.2 PROPIEDADES DE LA FUNCIÓN GAMMA

A lo largo del capítulo necesitaremos ciertas propiedades básicas de la función $\Gamma(s)$. Las citamos a continuación para fácil referencia, si bien no las precisaremos todas. Las demostraciones se pueden encontrar en gran número de textos relativos a la teoría de las funciones de variable compleja.

Para $\sigma > 0$ tenemos la representación integral

$$(1) \quad \Gamma(s) = \int_0^{\infty} x^{s-1} e^{-x} dx.$$

La función definida de esta forma para $\sigma > 0$ se puede prolongar al otro lado de la recta $\sigma = 0$, y $\Gamma(s)$ existe como función de s y es analítica en todo el plano complejo salvo para polos simples en los puntos

$$s = 0, -1, -2, -3, \dots,$$

con residuo $(-1)^n/n!$ en $s = -n$. Tenemos además la representación

$$\Gamma(s) = \lim_{n \rightarrow \infty} \frac{n! n^s}{s(s+1) \cdots (s+n)} \quad \text{para } s \neq 0, -1, -2, \dots,$$

y la fórmula producto

$$\frac{1}{\Gamma(s)} = se^{Cs} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-s/n} \quad \text{para todo } s,$$

en donde C es la constante de Euler. Como el producto converge para todo s , $\Gamma(s)$ nunca vale cero. La función gamma satisface dos ecuaciones funcionales

$$(2) \quad \Gamma(s+1) = s\Gamma(s)$$

y

$$(3) \quad \Gamma(s)\Gamma(1-s) = \frac{\pi}{\operatorname{sen} \pi s},$$

válidas para todo s , y una fórmula de multiplicación

$$(4) \quad \Gamma(s)\Gamma\left(s + \frac{1}{m}\right) \cdots \Gamma\left(s + \frac{m-1}{m}\right) = (2\pi)^{(m-1)/2} m^{(1/2)-ms} \Gamma(ms),$$

válida para todo s y todo entero $m \geq 1$.

Utilizaremos la representación integral (1), las ecuaciones funcionales (2) y (3), y el hecho de que $\Gamma(s)$ existe en todo el plano con polos simples en los enteros $s = 0, -1, -2, \dots$. Observamos además que $\Gamma(n+1) = n!$ si n es un entero no negativo.

12.3 REPRESENTACIÓN INTEGRAL PARA LA FUNCIÓN ZETA DE HURWITZ

La función zeta de Hurwitz $\zeta(s, a)$ se halla inicialmente definida para $\sigma > 1$ por la serie

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}.$$

Teorema 12.1 *La serie que define $\zeta(s, a)$ converge absolutamente para $\sigma > 1$. La convergencia es uniforme en cada semiplano $\sigma \geq 1 + \delta$, $\delta > 0$, luego $\zeta(s, a)$ es una función analítica de s en el semiplano $\sigma > 1$.*

DEMOSTRACIÓN. Todas estas afirmaciones se siguen de las desigualdades

$$\sum_{n=1}^{\infty} |(n+a)^{-s}| = \sum_{n=1}^{\infty} (n+a)^{-\sigma} \leq \sum_{n=1}^{\infty} (n+a)^{-(1+\delta)}. \quad \square$$

Teorema 12.2 Para $\sigma > 1$ tenemos la representación integral

$$(5) \quad \Gamma(s)\zeta(s, a) = \int_0^{\infty} \frac{x^{s-1} e^{-ax}}{1 - e^{-x}} dx.$$

En particular, cuando $a = 1$, tenemos

$$\Gamma(s)\zeta(s) = \int_0^{\infty} \frac{x^{s-1} e^{-x}}{1 - e^{-x}} dx.$$

DEMOSTRACIÓN. En primer lugar hacemos s real, $s > 1$, y entonces extendemos el resultado a todo s complejo por prolongación analítica.

En la integral dada para $\Gamma(s)$ efectuamos el cambio de variable $x = (n+a)t$, en donde $n \geq 0$, para obtener

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1} dx = (n+a)^s \int_0^{\infty} e^{-(n+a)t} t^{s-1} dt,$$

o

$$(n+a)^{-s} \Gamma(s) = \int_0^{\infty} e^{-nt} e^{-at} t^{s-1} dt.$$

Sumando respecto a todos los $n \geq 0$ obtenemos

$$\zeta(s, a) \Gamma(s) = \sum_{n=0}^{\infty} \int_0^{\infty} e^{-nt} e^{-at} t^{s-1} dt,$$

siendo la serie de la derecha convergente si $\sigma > 1$. Ahora deseamos intercambiar la suma y la integral. La manera más simple para justificarlo consiste en considerar la integral como de Lebesgue. Puesto que el integrando es no negativo, el teorema de convergencia de Levi (teorema 10.25 de la referencia [2]) nos dice que la serie

$$\sum_{n=0}^{\infty} e^{-nt} e^{-at} t^{s-1}$$

converge casi para todo t hacia una función suma que es integrable de Lebesgue en $[0, +\infty)$ y que

$$\zeta(s, a)\Gamma(s) = \sum_{n=0}^{\infty} \int_0^{\infty} e^{-nt} e^{-at} t^{s-1} dt = \int_0^{\infty} \sum_{n=0}^{\infty} e^{-nt} e^{-at} t^{s-1} dt.$$

Pero si $t > 0$ tenemos $0 < e^{-t} < 1$ y entonces

$$\sum_{n=0}^{\infty} e^{-nt} = \frac{1}{1 - e^{-t}},$$

en donde la serie es geométrica. Por consiguiente tenemos

$$\sum_{n=0}^{\infty} e^{-nt} e^{-at} t^{s-1} = \frac{e^{-at} t^{s-1}}{1 - e^{-t}}$$

casi para todo t en $(0, +\infty)$, de hecho para todo t salvo en 0, luego

$$\zeta(s, a)\Gamma(s) = \int_0^{\infty} \sum_{n=0}^{\infty} e^{-nt} e^{-at} t^{s-1} dt = \int_0^{\infty} \frac{e^{-at} t^{s-1}}{1 - e^{-t}} dt.$$

Esto prueba (5) para s real > 1 . Para extender este resultado a todo número complejo s con $\sigma > 1$ observamos que ambos miembros son analíticos para $\sigma > 1$. Para demostrar que el miembro de la derecha es analítico suponemos $1 + \delta \leq \sigma \leq c$, en donde $c > 1$ y $\delta > 0$ y escribimos

$$\int_0^{\infty} \left| \frac{e^{-at} t^{s-1}}{1 - e^{-t}} \right| dt \leq \int_0^{\infty} \frac{e^{-at} t^{\sigma-1}}{1 - e^{-t}} dt = \left(\int_0^1 + \int_1^{\infty} \right) \frac{e^{-at} t^{\sigma-1}}{1 - e^{-t}} dt.$$

Si $0 \leq t \leq 1$ tenemos $t^{\sigma-1} \leq t^{\delta}$, y, si $t \geq 1$, tenemos $t^{\sigma-1} \leq t^{c-1}$. Además, como $e^{\delta} - 1 \geq t$ para $t \geq 0$ tenemos

$$\int_0^1 \frac{e^{-at} t^{\sigma-1}}{1 - e^{-t}} dt \leq \int_0^1 \frac{e^{(1-a)t} t^{\delta}}{e^t - 1} dt \leq e^{(1-a)} \int_0^1 t^{\delta-1} dt = \frac{e^{1-a}}{\delta},$$

y

$$\int_1^{\infty} \frac{e^{-at} t^{\sigma-1}}{1 - e^{-t}} dt \leq \int_1^{\infty} \frac{e^{-at} t^{c-1}}{1 - e^{-t}} dt \leq \int_0^{\infty} \frac{e^{-at} t^{c-1}}{1 - e^{-t}} dt = \Gamma(c)\zeta(c, a).$$

Esto prueba que la integral de (5) converge uniformemente en cada intervalo $1 + \delta \leq \sigma \leq c$, en donde $\delta > 0$, y por consiguiente representa una función analítica en cada intervalo, por lo tanto también la representa en el semiplano $\sigma > 1$. Por consiguiente, por prolongación analítica, (5) se verifica para todo s con $\sigma > 1$. $\square$

12.4 UNA REPRESENTACIÓN DE LA FUNCIÓN ZETA DE HURWITZ MEDIANTE UNA INTEGRAL DE CONTORNO

Para extender $\zeta(s, a)$ al otro lado de la recta $\sigma = 1$ deducimos otra representación, en términos de una integral de contorno. El contorno C es un lazo en torno del eje real negativo, tal como se indica en la figura 12.1. El lazo está compuesto de tres partes C_1 , C_2 , C_3 . C_2 es una circunferencia de radio $c < 2\pi$, orientada positivamente, con centro en el origen, y C_1 y C_3 son los lados superior e inferior de un «corte» en el plano complejo a lo largo del eje real negativo, recorrido tal como indica la figura 12.1.

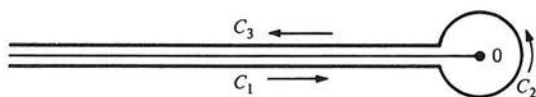


Figura 12.1

Esto significa que, sobre C_1 , utilizamos la parametrización $z = re^{-\pi i}$ y, sobre C_3 , $z = re^{\pi i}$, en donde r varía de c a $+\infty$.

Teorema 12.3 Si $0 < a \leq 1$, la función definida por la integral de contorno

$$I(s, a) = \frac{1}{2\pi i} \int_C \frac{z^{s-1} e^{az}}{1 - e^z} dz$$

es una función entera de s . Además, tenemos

$$\zeta(s, a) = \Gamma(1 - s)I(s, a) \quad \text{si } \sigma > 1.$$

DEMOSTRACIÓN. Aquí z^s significa $r^s e^{-\pi i s}$ sobre C_1 y $r^s e^{\pi i s}$ sobre C_3 . Consideramos un disco compacto arbitrario $|s| \leq M$ y vemos que las integrales a lo largo de C_1 y C_3 convergen uniformemente en tal disco. Al ser el integrando una función entera de s tenemos que $I(s, a)$ es una función entera.

A lo largo de C_1 tenemos, para $r \geq 1$,

$$|z^{s-1}| = r^{\sigma-1} |e^{-\pi i(\sigma-1+it)}| = r^{\sigma-1} e^{\pi t} \leq r^{M-1} e^{\pi M}$$

ya que $|s| \leq M$. Análogamente, a lo largo de C_3 tenemos, para $r \geq 1$,

$$|z^{s-1}| = r^{\sigma-1} |e^{\pi i(\sigma-1+it)}| = r^{\sigma-1} e^{-\pi t} \leq r^{M-1} e^{\pi M}.$$

Por lo tanto sobre C_1 y sobre C_3 tenemos, para $r \geq 1$,

$$\left| \frac{z^{s-1} e^{az}}{1 - e^z} \right| \leq \frac{r^{M-1} e^{\pi M} e^{-ar}}{1 - e^{-r}} = \frac{r^{M-1} e^{\pi M} e^{(1-a)r}}{e^r - 1}.$$

Pero $e^r - 1 > e^r/2$ cuando $r > \log 2$, luego el integrando está acotado por $A r^{M-1} e^{-ar}$, en donde A es una constante que depende de M pero no depende de r . Puesto que $\int_0^\infty r^{M-1} e^{-ar} dr$ converge si $c > 0$ hemos demostrado que las integrales a lo largo de C_1 y de C_3 convergen uniformemente sobre cada disco compacto $|s| \leq M$, y por lo tanto que $I(s, a)$ es una función entera de s .

Para probar (6) escribimos

$$2\pi i I(s, a) = \left(\int_{C_1} + \int_{C_2} + \int_{C_3} \right) z^{s-1} g(z) dz$$

en donde $g(z) = e^{az}/(1 - e^z)$. Sobre C_1 y C_3 tenemos $g(z) = g(-r)$, y sobre C_2 escribimos $z = ce^{i\theta}$, en donde $-\pi \leq \theta \leq \pi$. Esto nos proporciona

$$\begin{aligned} 2\pi i I(s, a) &= \int_0^c r^{s-1} e^{-\pi i s} g(-r) dr + i \int_{-\pi}^{\pi} c^{s-1} e^{(s-1)i\theta} c e^{i\theta} g(c e^{i\theta}) d\theta \\ &\quad + \int_c^\infty r^{s-1} e^{\pi i s} g(-r) dr \\ &= 2i \operatorname{sen}(\pi s) \int_c^\infty r^{s-1} g(-r) dr + i c^s \int_{-\pi}^{\pi} e^{is\theta} g(c e^{i\theta}) d\theta. \end{aligned}$$

Si dividimos por $2i$, obtenemos

$$\pi I(s, a) = \operatorname{sen}(\pi s) I_1(s, c) + I_2(s, c)$$

Ahora hacemos que $c \rightarrow 0$. Obtenemos

$$\lim_{c \rightarrow 0} I_1(s, c) = \int_0^\infty \frac{r^{s-1} e^{-ar}}{1 - e^{-r}} dr = \Gamma(s) \zeta(s, a),$$

si $\sigma > 1$. A continuación vemos que $\lim_{c \rightarrow 0} I_2(s, c) = 0$. Para ello observamos que $g(z)$ es analítica en $|z| < 2\pi$ excepto en un polo de primer orden en $z = 0$. Por consiguiente $zg(z)$ es analítica por todo el interior de $|z| < 2\pi$ y por lo tanto acotada a él, es decir $|g(z)| \leq A/|z|$, en donde $|z| = c < 2\pi$ y A es constante. Por consiguiente tenemos

$$|I_2(s, c)| \leq \frac{c^\sigma}{2} \int_{-\pi}^{\pi} e^{-t\theta} \frac{A}{c} d\theta \leq Ae^{\pi|t|} c^{\sigma-1}.$$

Si $\sigma > 1$ y $c \rightarrow 0$ obtenemos que $I_2(s, c) \rightarrow 0$, luego $\pi I(s, a) = \text{sen}(\pi s) \Gamma(s) \zeta(s, a)$. Como $\Gamma(s) \Gamma(1-s) = \pi / \text{sen} \pi s$ hemos demostrado (6). $\square$

12.5 LA PROLONGACIÓN ANALÍTICA DE LA FUNCIÓN ZETA DE HURWITZ

En la ecuación $\zeta(s, a) = \Gamma(1-s) I(s, a)$ válida para $\sigma > 1$, las funciones $I(s, a)$ y $\Gamma(1-s)$ son significativas para cada complejo s . Por consiguiente podemos utilizar esta ecuación para definir $\zeta(s, a)$ para $\sigma \leq 1$.

Definición. Si $\sigma \leq 1$ definimos $\zeta(s, a)$ por medio de la ecuación

$$(7) \quad \zeta(s, a) = \Gamma(1-s) I(s, a).$$

Esta ecuación proporciona la prolongación analítica de $\zeta(s, a)$ en el plano s entero.

Teorema 12.4 *La función $\zeta(s, a)$ definida de esta forma es analítica para todo s excepto en un polo simple en $s = 1$ con residuo 1.*

DEMOSTRACIÓN. Puesto que $I(s, a)$ es entera las únicas singularidades posibles de $\zeta(s, a)$ son los polos de $\Gamma(1-s)$, esto es, los puntos $s = 1, 2, 3, \dots$. Pero el teorema 12.1 prueba que $\zeta(s, a)$ es analítica en $s = 2, 3, \dots$, luego $s = 1$ es el único polo posible de $\zeta(s, a)$.

Ahora veremos que en $s = 1$ posee un polo con residuo 1. Si s es un entero, $s = n$, el integrando de la integral de contorno de $I(s, a)$ tomará el mismo valor sobre C_1 que sobre C_3 y por lo tanto las integrales a lo largo de C_1 y de C_3 se simplificarán, quedando

$$I(n, a) = \frac{1}{2\pi i} \int_{C_2} \frac{z^{n-1} e^{az}}{1 - e^z} dz = \text{Res}_{z=0} \frac{z^{n-1} e^{az}}{1 - e^z}.$$

En particular cuando $s = 1$ tenemos

$$I(1, a) = \operatorname{Res}_{z=0} \frac{e^{az}}{1 - e^z} = \lim_{z \rightarrow 0} \frac{ze^{az}}{1 - e^z} = \lim_{z \rightarrow 0} \frac{z}{1 - e^z} = \lim_{z \rightarrow 0} \frac{-1}{e^z} = -1.$$

Para calcular el residuo de $\zeta(s, a)$ en $s = 1$ calculamos el límite

$$\begin{aligned} \lim_{s \rightarrow 1} (s-1)\zeta(s, a) &= - \lim_{s \rightarrow 1} (1-s)\Gamma(1-s)I(s, a) = -I(1, a) \lim_{s \rightarrow 1} \Gamma(2-s) \\ &= \Gamma(1) = 1. \end{aligned}$$

Esto demuestra que $\zeta(s, a)$ tiene un polo simple en $s = 1$ con residuo 1. $\square$

Nota. Como $\zeta(s, a)$ es analítica en $s = 2, 3, \dots$ y $\Gamma(1-s)$ tiene polos en dichos puntos, la ecuación (7) implica que $I(s, a)$ debe anularse en estos puntos.

12.6 PROLONGACIÓN ANALÍTICA DE $\zeta(s)$ Y $L(s, \chi)$

En la introducción probábamos que, para $\sigma > 1$, se tenía

$$\zeta(s) = \zeta(s, 1)$$

y

$$(8) \quad L(s, \chi) = k^{-s} \sum_{r=1}^k \chi(r) \zeta\left(s, \frac{r}{k}\right),$$

en donde χ es un carácter de Dirichlet mod k . Utilizamos ahora estas fórmulas como *definiciones* de las funciones $\zeta(s)$ y $L(s, \chi)$ para $\sigma \leq 1$. De esta forma obtenemos la prolongación analítica de $\zeta(s)$ y de $L(s, \chi)$ al otro lado de la recta $\sigma=1$.

Teorema 12.5 (a) La función zeta de Riemann $\zeta(s)$ es analítica para todo s salvo en un polo simple en $s = 1$ con residuo 1.

(b) Para el carácter principal χ_1 mod k , la L -función $L(s, \chi_1)$ es analítica para todo s salvo para un polo simple en $s = 1$ con residuo $\varphi(k)/k$.

(c) Si $\chi \neq \chi_1$, $L(s, \chi)$ es una función entera de s .

DEMOSTRACIÓN. La parte (a) se sigue inmediatamente del teorema 12.4. Para probar (b) y (c) utilizamos la relación

$$\sum_{r \bmod k} \chi(r) = \begin{cases} 0 & \text{si } \chi \neq \chi_1, \\ \varphi(k) & \text{si } \chi = \chi_1. \end{cases}$$

Como $\zeta(s, r/k)$ tiene un polo simple en $s = 1$ con residuo 1, la función $\chi(r)\zeta(s, r/k)$ tiene un polo simple en $s = 1$ con residuo $\chi(r)$. Por consiguiente

$$\begin{aligned} \operatorname{Res}_{s=1} L(s, \chi) &= \lim_{s \rightarrow 1} (s-1)L(s, \chi) = \lim_{s \rightarrow 1} (s-1)k^{-s} \sum_{r=1}^k \chi(r)\zeta\left(s, \frac{r}{k}\right) \\ &= \frac{1}{k} \sum_{r=1}^k \chi(r) = \begin{cases} 0 & \text{si } \chi \neq \chi_1, \\ \frac{\varphi(k)}{k} & \text{si } \chi = \chi_1. \end{cases} \quad \square \end{aligned}$$

12.7 LA FÓRMULA DE HURWITZ PARA $\zeta(s, a)$

La función $\zeta(s, a)$ originalmente se definió para $\sigma > 1$, mediante una serie infinita. Hurwitz obtuvo otra representación en serie de $\zeta(s, a)$ válida en el semiplano $\sigma < 0$. Antes de establecer esta fórmula discutiremos un lema que se utilizará en su demostración.

Lema 1 $S(r)$ designa la región que queda cuando quitamos del z -plano todos los discos circulares abiertos de radio r , $0 < r < \pi$, con centros en los puntos $z = 2n\pi i$, $n = 0, \pm 1, \pm 2, \dots$ Entonces, si $0 < a \leq 1$, la función

$$g(z) = \frac{e^{az}}{1 - e^z}$$

está acotada en $S(r)$. (La cota depende de r .)

DEMOSTRACIÓN. Escribimos $z = x + iy$ y consideramos el rectángulo agujereado

$$Q(r) = \{z : |x| \leq 1, |y| \leq \pi, |z| \geq r\},$$

dibujado en la figura 12.2.

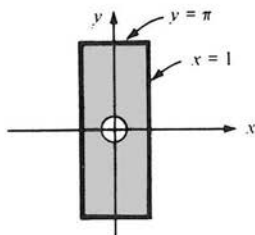


Figura 12.2

Este es un conjunto compacto, luego g está acotada en $Q(r)$. Además, puesto que $|g(z + 2\pi i)| = |g(z)|$, g está acotada en la banda con infinitos agujeros

$$\{z : |x| \leq 1, |z - 2n\pi i| \geq r, n = 0, \pm 1, \pm 2, \dots\}.$$

Ahora demostraremos que g está acotada en el exterior de esta banda. Suponemos $|x| \geq 1$ y consideramos

$$|g(z)| = \left| \frac{e^{az}}{1 - e^z} \right| = \frac{e^{ax}}{|1 - e^z|} \leq \frac{e^{ax}}{|1 - e^x|}.$$

Para $x \geq 1$ tenemos $|1 - e^x| = e^x - 1$ y $e^{ax} \leq e^x$, por lo tanto

$$|g(z)| \leq \frac{e^x}{e^x - 1} = \frac{1}{1 - e^{-x}} \leq \frac{1}{1 - e^{-1}} = \frac{e}{e - 1}.$$

Además, cuando $x \leq -1$ tenemos $|1 - e^x| = 1 - e^x$, por lo tanto

$$|g(z)| \leq \frac{e^{ax}}{1 - e^x} \leq \frac{1}{1 - e^x} \leq \frac{1}{1 - e^{-1}} = \frac{e}{e - 1}.$$

Por consiguiente $|g(z)| \leq e/(e - 1)$ para $|x| \geq 1$ y la demostración del lema queda terminada. $\square$

Ahora volvemos a la fórmula de Hurwitz. Ésta contiene otra serie de Dirichlet $F(x, s)$ dada por

$$(9) \quad F(x, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s},$$

en donde x es real y $\sigma > 1$. Obsérvese que $F(s, x)$ es una función periódica en x de período 1 y que $F(1, s) = \zeta(s)$. La serie converge absolutamente si $\sigma > 1$. Si x no es entero la serie converge también (condicionalmente) para $\sigma > 0$ ya que, para cada x fijo no entero, los coeficientes poseen sumas parciales acotadas.

Nota. Nos referiremos a $F(x, s)$ llamándola *función zeta periódica*.

Teorema 12.6 Fórmula de Hurwitz. Si $0 < a \leq 1$ y $\sigma > 1$ tenemos

$$(10) \quad \zeta(1 - s, a) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi i s/2} F(a, s) + e^{\pi i s/2} F(-a, s)\}.$$

Si $a \neq 1$ esta representación es válida también para $\sigma > 0$.

DEMOSTRACIÓN. Consideremos la función

$$I_N(s, a) = \frac{1}{2\pi i} \int_{C(N)} \frac{z^{s-1} e^{az}}{1 - e^z} dz,$$

en donde $C(N)$ es el contorno descrito en la figura 12.3, y N es un entero.

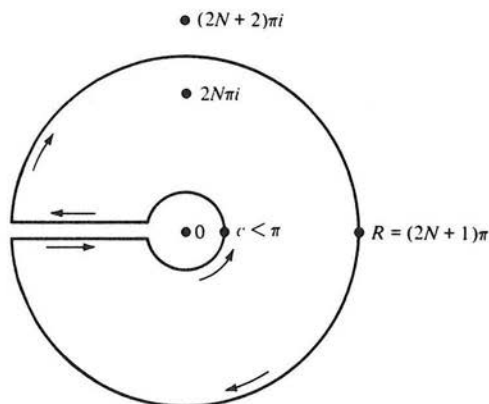


Figura 12.3

En primer lugar vemos que $\lim_{N \rightarrow \infty} I_N(s, a) = I(s, a)$ si $\sigma < 0$. Para ello es suficiente probar que la integral a lo largo de la circunferencia exterior tiende a 0 cuando $N \rightarrow \infty$.

Sobre la circunferencia exterior tenemos $z = Re^{i\theta}$, $-\pi \leq \theta \leq \pi$, luego

$$|z^{s-1}| = |R^{s-1} e^{i\theta(s-1)}| = R^{\sigma-1} e^{-t\theta} \leq R^{\sigma-1} e^{\pi|t|}.$$

Pero la circunferencia exterior pertenece al conjunto $S(r)$ del lema 1, por lo que el integrando está acotado por $Ae^{\pi|t|} R^{\sigma-1}$, en donde A es la cota de $|g(z)|$ introducida en el lema 1; luego la integral está acotada por

$$2\pi A e^{\pi|t|} R^{\sigma},$$

que $\rightarrow 0$ cuando $R \rightarrow \infty$ si $\sigma < 0$. Por consiguiente, si reemplazamos s por $1-s$ vemos que

$$(11) \quad \lim_{N \rightarrow \infty} I_N(1-s, a) = I(1-s, a) \quad \text{si } \sigma > 1.$$

Ahora calculamos $I_N(1-s, a)$ explícitamente mediante el teorema de residuos de Cauchy. Tenemos

$$I_N(1-s, a) = - \sum_{\substack{n=-N \\ n \neq 0}}^N R(n) = - \sum_{n=1}^N \{R(n) + R(-n)\}$$

en donde

$$R(n) = \operatorname{Res}_{z=2n\pi i} \left(\frac{z^{-s} e^{az}}{1-e^z} \right).$$

Ahora bien

$$R(n) = \lim_{z \rightarrow 2n\pi i} (z - 2n\pi i) \frac{z^{-s} e^{az}}{1-e^z} = \frac{e^{2n\pi i a}}{(2n\pi i)^s} \lim_{z \rightarrow 2n\pi i} \frac{z - 2n\pi i}{1-e^z} = - \frac{e^{2n\pi i a}}{(2n\pi i)^s},$$

luego

$$I_N(1-s, a) = \sum_{n=1}^N \frac{e^{2n\pi i a}}{(2n\pi i)^s} + \sum_{n=1}^N \frac{e^{-2n\pi i a}}{(-2n\pi i)^s}.$$

Pero $i^{-s} = e^{-\pi i s/2}$ y $(-1)^{-s} = e^{\pi i s/2}$, luego

$$I_N(1-s, a) = \frac{e^{-\pi i s/2}}{(2\pi)^s} \sum_{n=1}^N \frac{e^{2n\pi i a}}{n^s} + \frac{e^{\pi i s/2}}{(2\pi)^s} \sum_{n=1}^N \frac{e^{-2n\pi i a}}{n^s}.$$

Si hacemos que $N \rightarrow \infty$ y utilizamos (11) obtenemos

$$I(1-s, a) = \frac{e^{-\pi i s/2}}{(2\pi)^s} F(a, s) + \frac{e^{\pi i s/2}}{(2\pi)^s} F(-a, s).$$

Luego

$$\zeta(1-s, a) = \Gamma(s) I(1-s, a) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi i s/2} F(a, s) + e^{\pi i s/2} F(-a, s)\}. \quad \square$$

12.8 LA ECUACIÓN FUNCIONAL PARA LA FUNCIÓN ZETA DE RIEMANN

La primera aplicación de la fórmula de Hurwitz es la ecuación funcional de Riemann para $\zeta(s)$.

Teorema 12.7 Para todo s tenemos

$$(12) \quad \zeta(1-s) = 2(2\pi)^{-s} \Gamma(s) \cos\left(\frac{\pi s}{2}\right) \zeta(s)$$

o, lo que es equivalente,

$$(13) \quad \zeta(s) = 2(2\pi)^{s-1} \Gamma(1-s) \sin\left(\frac{\pi s}{2}\right) \zeta(1-s).$$

DEMOSTRACIÓN. Hacemos $a = 1$ en la fórmula de Hurwitz y obtenemos, para $\sigma > 1$,

$$\zeta(1-s) = \frac{\Gamma(s)}{(2\pi)^s} \{e^{-\pi i s/2} \zeta(s) + e^{\pi i s/2} \zeta(s)\} = \frac{\Gamma(s)}{(2\pi)^s} 2 \cos\left(\frac{\pi s}{2}\right) \zeta(s).$$

Esto prueba (12) para $\sigma > 1$ y el resultado se verifica para todo s por prolongación analítica. Para deducir (13) de (12) reemplazamos s por $1-s$. $\square$

Nota. Hacemos $s = 2n + 1$ en (12) en donde $n = 1, 2, 3, \dots$ y entonces el factor $\cos(\pi s/2)$ se anula y obtenemos los llamados *ceros triviales* de $\zeta(s)$,

$$\zeta(-2n) = 0 \quad \text{para } n = 1, 2, 3, \dots$$

La ecuación funcional se puede expresar de forma más sencilla utilizando la fórmula de duplicación de Legendre relativa a la función gamma.

$$2\pi^{1/2} 2^{-2s} \Gamma(2s) = \Gamma(s) \Gamma\left(s + \frac{1}{2}\right),$$

que es el caso especial $m = 2$ de la ecuación (4). Si sustituimos s por $(1-s)/2$, ésta se transforma en

$$2^s \pi^{1/2} \Gamma(1-s) = \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right).$$

Pero

$$\Gamma\left(\frac{s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right) = \frac{\pi}{\sin \frac{\pi s}{2}}$$

nos la transforma en

$$\Gamma(1-s) \sin \frac{\pi s}{2} = \frac{2^{-s} \pi^{1/2} \Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}.$$

Este resultado lo utilizamos para substituirlo en el producto $\Gamma(1-s) \sin(\pi s/2)$ de (13) y obtenemos

$$\pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s).$$

Con otras palabras, la ecuación funcional toma la forma

$$\Phi(s) = \Phi(1-s),$$

en donde

$$\Phi(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

La función $\Phi(s)$ tiene polos simples en $s=0$ y en $s=1$. Siguiendo a Riemann, multiplicamos $\Phi(s)$ por $s(s-1)/2$ para quitar los polos y definimos

$$\xi(s) = \frac{1}{2} s(s-1) \Phi(s).$$

Entonces $\xi(s)$ es una función entera de s y satisface la ecuación funcional

$$\xi(s) = \xi(1-s).$$

12.9 UNA ECUACIÓN FUNCIONAL PARA LA FUNCIÓN ZETA DE HURWITZ

La ecuación funcional para $\zeta(s)$ es un caso especial de una ecuación funcional para $\zeta(s, a)$ cuando a es racional.

Teorema 12.8 Si h y k son enteros, $1 \leq h \leq k$, entonces para todo s tenemos

$$(14) \quad \zeta\left(1-s, \frac{h}{k}\right) = \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^k \cos\left(\frac{\pi s}{2} - \frac{2\pi r h}{k}\right) \zeta\left(s, \frac{r}{k}\right).$$

DEMOSTRACIÓN. Este resultado se obtiene del hecho de que la función $F(x, s)$ es una combinación lineal de funciones zeta de Hurwitz cuando x es racional. En efecto, si $x = h/k$, podemos cambiar el orden de los términos de (9) de acuerdo con las clases de restos mod k y escribir

$$n = qk + r, \text{ en donde } 1 \leq r \leq k \text{ y } q = 0, 1, 2, \dots$$

Esto nos da, para $\sigma > 1$,

$$\begin{aligned} F\left(\frac{h}{k}, s\right) &= \sum_{n=1}^{\infty} \frac{e^{2\pi i n h/k}}{n^s} = \sum_{r=1}^k \sum_{q=0}^{\infty} \frac{e^{2\pi i r h/k}}{(qk+r)^s} = \frac{1}{k^s} \sum_{r=1}^k e^{2\pi i r h/k} \sum_{q=0}^{\infty} \frac{1}{\left(q + \frac{r}{k}\right)^s} \\ &= k^{-s} \sum_{r=1}^k e^{2\pi i r h/k} \zeta\left(s, \frac{r}{k}\right). \end{aligned}$$

Por consiguiente, si hacemos $a = h/k$ en la fórmula de Hurwitz obtenemos

$$\begin{aligned} \zeta\left(1-s, \frac{h}{k}\right) &= \frac{\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^k (e^{-\pi i s/2} e^{2\pi i r h/k} + e^{\pi i s/2} e^{-2\pi i r h/k}) \zeta\left(s, \frac{r}{k}\right) \\ &= \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^k \cos\left(\frac{\pi s}{2} - \frac{2\pi r h}{k}\right) \zeta\left(s, \frac{r}{k}\right), \end{aligned}$$

que prueba (14) para $\sigma > 1$. El resultado vale para todo s por prolongación analítica. $\square$

Conviene observar que cuando $h = k = 1$, sólo existe un término en la suma de (14) y se obtiene la ecuación funcional de Riemann.

12.10 LA ECUACIÓN FUNCIONAL PARA L -FUNCIONES

También podemos utilizar la fórmula de Hurwitz para deducir una ecuación funcional para las L -funciones de Dirichlet. En primer lugar probaremos que basta considerar solamente los caracteres primitivos mod k .

Teorema 12.9 *Sea χ un carácter de Dirichlet mod k , sea d un módulo inducido, y escribamos*

$$\chi(n) = \psi(n)\chi_1(n),$$

en donde ψ es un carácter mod d y χ_1 es el carácter principal mod k . Entonces, para todo s tenemos

$$L(s, \chi) = L(s, \psi) \prod_{p|k} \left(1 - \frac{\psi(p)}{p^s}\right).$$

DEMOSTRACIÓN. Primeramente hacemos $\sigma > 1$ y utilizamos el producto de Euler

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Al ser $\chi(p) = \psi(p)\chi_1(p)$ y $\chi_1(p) = 0$ si $p|k$ y $\chi_1(p) = 1$ si $p \nmid k$ obtenemos

$$\begin{aligned} L(s, \chi) &= \prod_{p \nmid k} \frac{1}{1 - \frac{\psi(p)}{p^s}} = \prod_p \frac{1}{1 - \frac{\psi(p)}{p^s}} \cdot \prod_{p|k} \left(1 - \frac{\psi(p)}{p^s}\right) \\ &= L(s, \psi) \prod_{p|k} \left(1 - \frac{\psi(p)}{p^s}\right). \end{aligned}$$

Esto prueba el teorema para $\sigma > 1$ y lo extendemos a todo s por prolongación analítica. $\square$

Nota. Si en el teorema anterior elegimos d de forma que sea el conductor de χ , entonces ψ es un carácter primitivo mod d . Esto prueba que cada L -serie $L(s, \chi)$ es igual a la L -serie $L(s, \psi)$ de un carácter primitivo, multiplicada por un número finito de factores.

Para deducir la ecuación funcional para L -funciones a partir de la fórmula de Hurwitz, ante todo expresaremos $L(s, \chi)$ en términos de la función zeta periódica $F(x, s)$.

Teorema 12.10 *Sea χ un carácter primitivo mod k . Entonces, para $\sigma > 1$, tenemos*

$$(15) \quad G(1, \bar{\chi})L(s, \chi) = \sum_{h=1}^k \bar{\chi}(h)F\left(\frac{h}{k}, s\right),$$

en donde $G(m, \chi)$ es la suma de Gauss asociada a χ ,

$$G(m, \chi) = \sum_{r=1}^k \chi(r)e^{2\pi i rm/k}.$$

DEMOSTRACIÓN. Hacemos $x = h/k$ en (9), multiplicamos por $\bar{\chi}(h)$, sumamos respecto de h y obtenemos

$$\begin{aligned} \sum_{h=1}^k \bar{\chi}(h)F\left(\frac{h}{k}, s\right) &= \sum_{h=1}^k \sum_{n=1}^{\infty} \bar{\chi}(h)e^{2\pi i nh/k} n^{-s} = \sum_{n=1}^{\infty} n^{-s} \sum_{h=1}^k \bar{\chi}(h)e^{2\pi i nh/k} \\ &= \sum_{n=1}^{\infty} n^{-s} G(n, \bar{\chi}). \end{aligned}$$

Pero $G(n, \bar{\chi})$ es separable puesto que $\bar{\chi}$ es primitivo, luego $G(n, \bar{\chi}) = \chi(n)G(1, \bar{\chi})$, luego

$$\sum_{h=1}^k \bar{\chi}(h)F\left(\frac{h}{k}, s\right) = G(1, \bar{\chi}) \sum_{n=1}^{\infty} \chi(n)n^{-s} = G(1, \bar{\chi})L(s, \chi). \quad \square$$

Teorema 12.11 *Ecuación funcional para L -funciones de Dirichlet. Si χ es un carácter primitivo mod k , entonces, para todo s , tenemos*

$$(16) \quad L(1-s, \chi) = \frac{k^{s-1}\Gamma(s)}{(2\pi)^s} \{e^{-\pi i s/2} + \chi(-1)e^{\pi i s/2}\} G(1, \chi)L(s, \bar{\chi}).$$

DEMOSTRACIÓN. Hacemos $x = h/k$ en la fórmula de Hurwitz, a continuación

multiplicamos cada miembro por $\chi(h)$ y sumamos respecto de h . Ello nos proporciona

$$\sum_{h=1}^k \chi(h) \zeta\left(1 - s, \frac{h}{k}\right) = \frac{\Gamma(s)}{(2\pi)^s} \left\{ e^{-\pi i s/2} \sum_{h=1}^k \chi(h) F\left(\frac{h}{k}, s\right) + e^{\pi i s/2} \sum_{h=1}^k \chi(h) F\left(\frac{-h}{k}, s\right) \right\}.$$

Como $F(x, s)$ es periódica en x de período 1 y $\chi(h) = \chi(-1)\chi(-h)$ podemos escribir

$$\begin{aligned} \sum_{h \bmod k} \chi(h) F\left(\frac{-h}{k}, s\right) &= \chi(-1) \sum_{h \bmod k} \chi(-h) F\left(\frac{-h}{k}, s\right) \\ &= \chi(-1) \sum_{h \bmod k} \chi(k-h) F\left(\frac{k-h}{k}, s\right) \\ &= \chi(-1) \sum_{h \bmod k} \chi(h) F\left(\frac{h}{k}, s\right), \end{aligned}$$

y la fórmula precedente se transforma en

$$\sum_{h=1}^k \chi(h) \zeta\left(1 - s, \frac{h}{k}\right) = \frac{\Gamma(s)}{(2\pi)^s} \{ e^{-\pi i s/2} + \chi(-1) e^{\pi i s/2} \} \sum_{h=1}^k \chi(h) F\left(\frac{h}{k}, s\right).$$

Ahora multiplicamos ambos miembros por k^{s-1} y utilizamos (15) para obtener (16). □

12.11 CÁLCULO DE $\zeta(-n, a)$

El valor de $\sigma(-n, a)$ se puede calcular de forma explícita si n es un entero no negativo. Tomamos $s = -n$ en la relación $\zeta(s, a) = \Gamma(1-s)I(s, a)$ y obtenemos

$$\zeta(-n, a) = \Gamma(1+n)I(-n, a) = n! I(-n, a).$$

Además tenemos

$$I(-n, a) = \operatorname{Res}_{z=0} \left(\frac{z^{-n-1} e^{az}}{1 - e^z} \right).$$

El cálculo de este residuo conduce a una clase interesante de funciones que se conocen con el nombre de *polinomios de Bernoulli*.

Definición. Para cada complejo x definimos la función $B_n(x)$ por la ecuación

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n, \text{ en donde } |z| < 2\pi.$$

Los números $B_n(0)$ se llaman números de Bernoulli y se designan B_n . Entonces

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n, \text{ en donde } |z| < 2\pi.$$

Teorema 12.12 Las funciones $B_n(x)$ son polinomios en x dados por

$$B_n(x) = \sum_{k=0}^n \binom{n}{k} B_k x^{n-k}.$$

DEMOSTRACIÓN. Tenemos

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n = \frac{z}{e^z - 1} \cdot e^{xz} = \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \right) \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n \right).$$

Igualando los coeficientes de z^n obtenemos

$$\frac{B_n(x)}{n!} = \sum_{k=0}^n \frac{B_k}{k!} \frac{x^{n-k}}{(n-k)!}$$

de donde se sigue el teorema.

Teorema 12.12 Para cada entero $n \geq 0$ tenemos

$$(17) \quad \zeta(-n, a) = -\frac{B_{n+1}(a)}{n+1}.$$

DEMOSTRACIÓN. Como ya hemos indicado anteriormente, tenemos $\zeta(-n, a) = n! I(-n, a)$. Ahora bien

$$\begin{aligned} I(-n, a) &= \operatorname{Res}_{z=0} \left(\frac{z^{-n-1} e^{az}}{1 - e^z} \right) = - \operatorname{Res}_{z=0} \left(z^{-n-2} \frac{z e^{az}}{e^z - 1} \right) \\ &= - \operatorname{Res}_{z=0} \left(z^{-n-2} \sum_{m=0}^{\infty} \frac{B_m(a)}{m!} z^m \right) = - \frac{B_{n+1}(a)}{(n+1)!}, \end{aligned}$$

de donde se obtiene (17). □

12.12 PROPIEDADES DE LOS NÚMEROS DE BERNOULLI Y DE LOS POLINOMIOS DE BERNOULLI

Teorema 12.14 *Los polinomios de Bernoulli $B_n(x)$ satisfacen la ecuación de diferencias*

$$(18) \quad B_n(x+1) - B_n(x) = nx^{n-1} \quad \text{si } n \geq 1.$$

Por consiguiente tenemos

$$(19) \quad B_n(0) = B_n(1) \quad \text{si } n \geq 2.$$

DEMOSTRACIÓN. Tenemos la identidad

$$z \frac{e^{(x+1)z}}{e^z - 1} - z \frac{e^{xz}}{e^z - 1} = ze^{xz}$$

de la que resulta

$$\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} z^n = \sum_{n=0}^{\infty} \frac{x^n}{n!} z^{n+1}.$$

Igualando los coeficientes de z^n obtenemos (18). Haciendo $x = 0$ en (18) se deduce (19). □

Teorema 12.15 *Si $n \geq 2$ tenemos*

$$B_n = \sum_{k=0}^n \binom{n}{k} B_k.$$

DEMOSTRACIÓN. Este resultado se obtiene haciendo $x = 1$ en el teorema 12.12 y utilizando (19). □

El teorema 12.15 nos proporciona una fórmula recurrente para calcular los números de Bernoulli. La definición nos da $B_0 = 1$, y el teorema 12.15 proporciona sucesivamente los valores

$$\begin{aligned} B_0 &= 1, & B_1 &= -\frac{1}{2}, & B_2 &= \frac{1}{6}, & B_3 &= 0, & B_4 &= -\frac{1}{30}, \\ B_5 &= 0, & B_6 &= \frac{1}{42}, & B_7 &= 0, & B_8 &= -\frac{1}{30}, & B_9 &= 0, \\ B_{10} &= \frac{5}{66}, & B_{11} &= 0. \end{aligned}$$

Conociendo los B_k podemos calcular los polinomios $B_n(x)$ utilizando el teorema 12.12. Los primeros son:

$$\begin{aligned} B_0(x) &= 1, & B_1(x) &= x - \frac{1}{2}, & B_2(x) &= x^2 - x + \frac{1}{6}, \\ B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, & B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30}. \end{aligned}$$

Observamos que los teoremas 12.12 y 12.15 se pueden escribir simbólicamente como sigue:

$$B_n(x) = (B + x)^n, \quad B_n = (B + 1)^n.$$

En estas fórmulas simbólicas los segundos miembros se desarrollan por el teorema del binomio y entonces cada potencia B^k se substituye por B_k .

Teorema 12.16 Si $n \geq 0$ tenemos

$$(20) \quad \zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

También, si $n \geq 1$ tenemos $\zeta(-2n) = 0$, por consiguiente $B_{2n+1} = 0$.

DEMOSTRACIÓN. Para calcular $\zeta(-n)$ basta tomar simplemente $a = 1$ en el teorema 12.13. Ya hemos observado que la ecuación funcional

$$(21) \quad \zeta(1-s) = 2(2\pi)^{-s} \Gamma(s) \cos\left(\frac{\pi s}{2}\right) \zeta(s)$$

implica $\zeta(-2n) = 0$ para $n \geq 1$, luego $B_{2n+1} = 0$ por (20). □

Nota. El resultado $B_{2n+1} = 0$ también se obtiene observando que el primer miembro de

$$\frac{z}{e^z - 1} + \frac{1}{2}z = 1 + \sum_{n=2}^{\infty} \frac{B_n}{n!} z^n$$

es una función par de z .

Teorema 12.17 Si k es un entero positivo tenemos

$$(22) \quad \zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k} B_{2k}}{2(2k)!}.$$

DEMOSTRACIÓN. Hacemos $s = 2k$ en la ecuación funcional de $\zeta(s)$ y se obtiene

$$\zeta(1 - 2k) = 2(2\pi)^{-2k} \Gamma(2k) \cos(\pi k) \zeta(2k),$$

o bien

$$-\frac{B_{2k}}{2k} = 2(2\pi)^{-2k} (2k - 1)! (-1)^k \zeta(2k).$$

Esto implica (22). □

Nota. Si hacemos $s = 2k + 1$ en (21) ambos miembros se anulan y carecemos de información acerca de $\zeta(2k + 1)$. Con todo se desconoce una fórmula simple análoga a (22) para $\zeta(2k + 1)$ e incluso para casos especiales tales como $\zeta(3)$. Tampoco se sabe cuando $\zeta(2k + 1)$ es racional o irracional para cada k .

Teorema 12.18 Los números de Bernoulli B_{2k} tienen signo alternativo. Es decir

$$(-1)^{k+1} B_{2k} > 0.$$

Además, $|B_{2k}| \rightarrow \infty$ cuando $k \rightarrow \infty$. De hecho,

$$(23) \quad (-1)^{k+1} B_{2k} \sim \frac{2(2k)!}{(2\pi)^{2k}} \text{ cuando } k \rightarrow \infty.$$

DEMOSTRACIÓN. Dado que $\zeta(2k) > 0$, (22) prueba que los números B_{2k} cambian de signo. La relación asintótica (23) se obtiene del hecho de que $\zeta(2k) \rightarrow 1$ cuando $k \rightarrow \infty$.

Nota. De (23) se obtiene $|B_{2k+2}/B_{2k}| \sim k^2/\pi^2$ cuando $k \rightarrow \infty$. Además, invocando la fórmula de Stirling, $n! \sim (n/e)^n \sqrt{2\pi n}$ obtenemos

$$(-1)^{k+1} B_{2k} \sim 4\pi \sqrt{e} \left(\frac{k}{\pi e}\right)^{2k+1/2} \quad \text{cuando } k \rightarrow \infty.$$

El teorema que sigue da el desarrollo de Fourier del polinomio $B_n(x)$ en el intervalo $0 < x \leq 1$.

Teorema 12.19 Si $0 < x \leq 1$ tenemos

$$(24) \quad B_n(x) = -\frac{n!}{(2\pi i)^n} \sum_{\substack{k=-\infty \\ k \neq 0}}^{+\infty} \frac{e^{2\pi i k x}}{k^n},$$

y entonces

$$B_{2n}(x) = (-1)^{n+1} \frac{2(2n)!}{(2\pi)^{2n}} \sum_{k=1}^{\infty} \frac{\cos 2\pi k x}{k^{2n}},$$

$$B_{2n+1}(x) = (-1)^{n+1} \frac{2(2n+1)!}{(2\pi)^{2n+1}} \sum_{k=1}^{\infty} \frac{\operatorname{sen} 2\pi k x}{k^{2n+1}}.$$

DEMOSTRACIÓN. La ecuación (24) se obtiene inmediatamente haciendo $s = n$ en la fórmula de Hurwitz y aplicando el teorema 12.13. Las otras dos fórmulas son casos especiales de (24). $\square$

Nota. La función $\bar{B}_n(x)$ definida para todo real x por el segundo miembro de (24) se llama *n-ésima función periódica de Bernoulli*. Es periódica de período 1 y coincide con el polinomio de Bernoulli $B_n(x)$ en el intervalo $0 < x \leq 1$. Entonces tenemos

$$\bar{B}_n(x) = B_n(x - [x]).$$

12.13 FÓRMULAS PARA $L(0, \chi)$

El teorema 12.13 implica

$$\zeta(0, a) = -B_1(a) = \frac{1}{2} - a.$$

En particular $\zeta(0) = \zeta(0, 1) = -1/2$. También podemos calcular $L(0, \chi)$ para cada carácter de Dirichlet χ .

Teorema 12.20 Sea χ un carácter cualquiera de Dirichlet mod k .

(a) Si $\chi = \chi_1$ (el carácter principal), entonces $L(0, \chi_1) = 0$.

(b) Si $\chi \neq \chi_1$ tenemos

$$L(0, \chi) = -\frac{1}{k} \sum_{r=1}^k r\chi(r).$$

Además, $L(0, \chi) = 0$ si $\chi(-1) = 1$.

DEMOSTRACIÓN. Si $\chi = \chi_1$ utilizamos la fórmula

$$L(s, \chi_1) = \zeta(s) \prod_{p|k} (1 - p^{-s})$$

demostrada para $\sigma > 1$ en el capítulo 11. También es válida para todo s por prolongación analítica. Cuando $s = 0$ el producto se anula, luego $L(0, \chi_1) = 0$.

Si $\chi \neq \chi_1$ tenemos

$$L(0, \chi) = \sum_{r=1}^k \chi(r) \zeta\left(0, \frac{r}{k}\right) = \sum_{r=1}^k \chi(r) \left(\frac{1}{2} - \frac{r}{k}\right) = -\frac{1}{k} \sum_{r=1}^k r\chi(r).$$

Ahora bien

$$\begin{aligned} \sum_{r=1}^k r\chi(r) &= \sum_{r=1}^k (k-r)\chi(k-r) = k \sum_{r=1}^k \chi(k-r) - \sum_{r=1}^k r\chi(-r) \\ &= -\chi(-1) \sum_{r=1}^k r\chi(r). \end{aligned}$$

Por consiguiente, si $\chi(-1) = 1$, tenemos $\sum_{r=1}^k r\chi(r) = 0$. □

12.14 APROXIMACIÓN DE $\zeta(s, a)$ POR MEDIO DE SUMAS FINITAS

Algunas aplicaciones requieren valorar el orden de crecimiento de $\zeta(\sigma + it, a)$ como función de t . Esto se deduce de otra representación de $\zeta(s, a)$ obtenida

de la fórmula de sumación de Euler. Esta relaciona $\zeta(s, a)$ con las sumas parciales de su serie en el semiplano $\sigma > 0$ y además proporciona otro camino para extender $\zeta(s, a)$ analíticamente al otro lado de la recta $\sigma = 1$.

Teorema 12.21 Para todo entero $N \geq 0$ y $\sigma > 0$ tenemos

$$(25) \quad \zeta(s, a) = \sum_{n=0}^N \frac{1}{(n+a)^s} + \frac{(N+a)^{1-s}}{s-1} - s \int_N^{\infty} \frac{x - [x]}{(x+a)^{s+1}} dx.$$

DEMOSTRACIÓN. Aplicando la fórmula de sumación de Euler (teorema 3.1) con $f(t) = (t+a)^{-s}$ y con x e y enteros, obtenemos

$$\sum_{y < n \leq x} \frac{1}{(n+a)^s} = \int_y^x \frac{dt}{(t+a)^s} - s \int_y^x \frac{t - [t]}{(t+a)^{s+1}} dt.$$

Tomando $y = N$ y haciendo que $x \rightarrow \infty$, y siempre $\sigma > 1$, obtenemos

$$\sum_{n=N+1}^{\infty} \frac{1}{(n+a)^s} = \int_N^{\infty} \frac{dt}{(t+a)^s} - s \int_N^{\infty} \frac{t - [t]}{(t+a)^{s+1}} dt,$$

luego

$$\zeta(s, a) - \sum_{n=0}^N \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - s \int_N^{\infty} \frac{t - [t]}{(t+a)^{s+1}} dt.$$

Esto prueba (25) para $\sigma > 1$. Si $\sigma \geq \delta > 0$ la integral se halla dominada por $\int_N^{\infty} (t+a)^{-\delta-1} dt$ por lo que es uniformemente convergente para $\sigma \geq \delta$ y por ende representa una función analítica en el semiplano $\sigma > 0$. Por consiguiente (25) se sigue cumpliendo para $\sigma > 0$ por prolongación analítica. $\square$

La integral de la derecha de (25) se puede escribir también como serie. Descomponemos la integral en suma de integrales en cada una de las cuales $[x]$ es constante, es decir $[x] = n$, y obtenemos

$$\int_N^{\infty} \frac{x - [x]}{(x+a)^{s+1}} dx = \sum_{n=N}^{\infty} \int_n^{n+1} \frac{x - n}{(x+a)^{s+1}} dx = \sum_{n=N}^{\infty} \int_0^1 \frac{u}{(u+n+a)^{s+1}} du.$$

Por consiguiente (25) también se puede escribir en la forma

$$(26) \quad \zeta(s, a) - \sum_{n=0}^N \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - s \sum_{n=N}^{\infty} \int_0^1 \frac{u}{(u+n+a)^{s+1}} du$$

si $\sigma > 0$. La integración por partes conduce a representaciones similares en sucesivos semiplanos cada vez más amplios, tal como indica el teorema que sigue.

Teorema 11.22 Si $\sigma > -1$ tenemos

$$(27) \quad \zeta(s, a) - \sum_{n=0}^N \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - \frac{s}{2!} \left\{ \zeta(s+1, a) - \sum_{n=0}^N \frac{1}{(n+a)^{s+1}} \right\} - \frac{s(s+1)}{2!} \sum_{n=N}^{\infty} \int_0^1 \frac{u^2}{(n+a+u)^{s+2}} du.$$

En general, si $\sigma > -m$, en donde $m = 1, 2, 3, \dots$, tenemos

$$(28) \quad \zeta(s, a) - \sum_{n=0}^N \frac{1}{(n+a)^s} = \frac{(N+a)^{1-s}}{s-1} - \sum_{r=1}^m \frac{s(s+1) \cdots (s+r-1)}{(r+1)!} \times \left\{ \zeta(s+r, a) - \sum_{n=0}^N \frac{1}{(n+a)^{s+r}} \right\} - \frac{s(s+1) \cdots (s+m)}{(m+1)!} \times \sum_{n=N}^{\infty} \int_0^1 \frac{u^{m+1}}{(n+a+u)^{s+m+1}} du.$$

DEMOSTRACIÓN. La integración por partes implica

$$\int \frac{u du}{(n+a+u)^{s+1}} = \frac{u^2}{2(n+a+u)^{s+1}} + \frac{s+1}{2} \int \frac{u^2 du}{(n+a+u)^{s+2}},$$

luego, si $\sigma > 0$, tenemos

$$\sum_{n=N}^{\infty} \int_0^1 \frac{u du}{(n+a+u)^{s+1}} = \frac{1}{2} \sum_{n=N}^{\infty} \frac{1}{(n+a+1)^{s+1}} + \frac{s+1}{2} \sum_{n=N}^{\infty} \int_0^1 \frac{u^2 du}{(n+a+u)^{s+2}}.$$

Pero, si $\sigma > 0$, la primera suma de la derecha es $\zeta(s+1, a) - \sum_{n=0}^N (n+a)^{-s-1}$ y (26) implica (27). El resultado también es válido para $\sigma > -1$ por prolongación analítica. Repitiendo la integración por partes obtenemos la representación más general dada por (28). $\square$

12.15 DESIGUALDADES PARA $|\zeta(s, a)|$

Las fórmulas de la sección anterior proporcionan cotas superiores para $|\zeta(\sigma+it, a)|$ como función de t .

Teorema 12.23 (a) Si $\delta > 0$ tenemos

$$(29) \quad |\zeta(s, a) - a^{-s}| \leq \zeta(1 + \delta) \quad \text{si } \sigma \geq 1 + \delta.$$

(b) Si $0 < \delta < 1$ existe una constante positiva $A(\delta)$, que depende de δ pero no de s ni de a , tal que

$$(30) \quad |\zeta(s, a) - a^{-s}| \leq A(\delta)|t|^\delta \quad \text{si } 1 - \delta \leq \sigma \leq 2 \text{ y } |t| \geq 1,$$

$$(31) \quad |\zeta(s, a) - a^{-s}| \leq A(\delta)|t|^{1+\delta} \quad \text{si } -\delta \leq \sigma \leq \delta \text{ y } |t| \geq 1,$$

$$(32) \quad |\zeta(s, a)| \leq A(\delta)|t|^{m+1+\delta} \quad \text{si } -m - \delta \leq \sigma \leq -m + \delta \text{ y } |t| \geq 1,$$

en donde $m = 1, 2, 3, \dots$

DEMOSTRACIÓN. Para la parte (a) utilizamos la serie que define $\zeta(s, a)$ y obtenemos

$$|\zeta(s, a) - a^{-s}| \leq \sum_{n=1}^{\infty} \frac{1}{(n+a)^\sigma} \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}} = \zeta(1 + \delta),$$

que implica (29).

Para la parte (b) utilizamos la representación de (25) cuando $1 - \delta \leq \sigma \leq 2$ a fin de obtener

$$\begin{aligned} |\zeta(s, a) - a^{-s}| &\leq \sum_{n=1}^N \frac{1}{(n+a)^\sigma} + \frac{(N+a)^{1-\sigma}}{|s-1|} + |s| \int_N^\infty \frac{dx}{(x+a)^{\sigma+1}} \\ &< 1 + \int_1^N \frac{dx}{(x+a)^\sigma} + \frac{(N+a)^{1-\sigma}}{|s-1|} + \frac{|s|}{\sigma} (N+a)^{-\sigma}. \end{aligned}$$

Puesto que $\sigma \geq 1 - \delta > 0$, tenemos $(x + a)^\sigma \geq (x + a)^{1-\delta} > x^{1-\delta}$ luego

$$\int_1^N \frac{dx}{(x+a)^\sigma} \leq \int_1^N \frac{dx}{x^{1-\delta}} < \frac{N^\delta}{\delta}.$$

Además, como $|s-1| = |\sigma-1+it| \geq |t| \geq 1$ tenemos

$$\frac{(N+a)^{1-\sigma}}{|s-1|} \leq (N+a)^\delta \leq (N+1)^\delta.$$

Finalmente, como $|s| \leq |\sigma| + |t| \leq 2 + |t|$ obtenemos

$$\frac{|s|}{\sigma} (N+a)^{-\sigma} < \frac{2+|t|}{1-\delta} (N+a)^{\delta-1} < \frac{2+|t|}{1-\delta} \frac{1}{N^{1-\delta}}.$$

Esto nos proporciona

$$|\zeta(s, a) - a^{-s}| < 1 + \frac{N^\delta}{\delta} + (N+1)^\delta + \frac{2+|t|}{1-\delta} \frac{N^\delta}{N}.$$

Ahora hacemos $N = 1 + [|t|]$. Entonces los últimos tres términos son $O(|t|^\delta)$, en los cuales la constante que aparece en el símbolo O depende únicamente de δ . Esto demuestra (30).

Para probar (31) utilizamos la representación de (27), que nos da

$$\begin{aligned} |\zeta(s, a) - a^{-s}| &\leq \sum_{n=1}^N \frac{1}{(n+a)^\sigma} + \frac{(N+a)^{1-\sigma}}{|s-1|} + \frac{1}{2} |s| \{ |\zeta(s+1, a) - a^{-s-1}| \} \\ &\quad + \frac{1}{2} |s| \sum_{n=1}^N \frac{1}{(n+a)^{\sigma+1}} + \frac{1}{2} |s| |s+1| \sum_{n=N}^{\infty} \frac{1}{(n+a)^{\sigma+2}}. \end{aligned}$$

Como en la demostración de (30), tomamos $N = 1 + [|t|]$, así que $N = O(|t|)$, y vemos que cada término de la derecha es $O(|t|^{1+\delta})$, y que la constante que aparece en el símbolo O depende únicamente de δ . Las desigualdades $1 - \delta \leq \sigma \leq 1 + \delta$, luego

$$\begin{aligned} \sum_{n=1}^N \frac{1}{(n+a)^\sigma} &< 1 + \int_1^N \frac{dx}{(x+a)^\sigma} < 1 + \frac{(N+a)^{1-\sigma}}{1-\sigma} \\ &\leq 1 + \frac{(N+1)^{1+\delta}}{1-\delta} = O(|t|^{1+\delta}). \end{aligned}$$

Como $|s-1| \geq |t| \geq 1$, el segundo miembro también es $O(|t|^{1+\delta})$. Para el tercer término utilizamos (30), observando que $1-\delta \leq \sigma+1 \leq 1+\delta$ y que $|s|=O(|t|)$, y vemos que este término también es $O(|t|^{1+\delta})$. Después, se obtiene

$$\begin{aligned} |s| \sum_{n=1}^N \frac{1}{(n+a)^{\sigma+1}} &= O\left(|t| \int_1^N \frac{dx}{(x+a)^{1-\delta}}\right) \\ &= O(|t|N^{-\delta}) = O(|t|^{1-\delta}) = O(|t|^{1+\delta}). \end{aligned}$$

Finalmente,

$$\begin{aligned} |s||s+1| \sum_{n=N}^{\infty} \frac{1}{(n+a)^{\sigma+2}} &= O\left(|t|^2 \int_N^{\infty} \frac{dx}{(x+a)^{\sigma+2}}\right) = O(|t|^2 N^{-\sigma-1}) \\ &= O(|t|^2 N^{\delta-1}) = O(|t|^{1+\delta}). \end{aligned}$$

Esto termina la demostración de (31).

La demostración de (32) es análoga, salvo que utilizamos (28) y observamos que $a^{-\sigma} = O(1)$ cuando $\sigma < 0$. $\square$

12.16 DESIGUALDADES PARA $|\zeta(s)|$ Y PARA $|L(s, \chi)|$

Cuando $a=1$ las acotaciones del teorema 12.23 dan las correspondientes acotaciones para $|\zeta(s)|$. Nos proporciona también cotas para las L -series de Dirichlet. Si $\sigma \geq 1+\delta$, en donde $\delta > 0$, tanto $|\zeta(s)|$ como $|L(s, \chi)|$ se hallan dominadas por $\zeta(1+\delta)$ por lo que únicamente consideramos $\sigma \leq 1+\delta$.

Teorema 12.24. *Sea χ un carácter de Dirichlet mod k y supongamos $0 < \delta < 1$. Entonces existe una constante positiva $A(\delta)$, que depende de δ pero no de s ni de k , tal que para $s = \sigma + it$ con $|t| \geq 1$ tenemos*

$$(33) \quad |L(s, \chi)| \leq A(\delta) |kt|^{m+1+\delta} \quad \text{si} \quad -m-\delta \leq \sigma-m+\delta,$$

en donde $m = -1, 0, 1, 2, \dots$

DEMOSTRACIÓN. Recordamos la relación

$$L(s, \chi) = k^{-s} \sum_{r=1}^{k-1} \chi(r) \zeta\left(s, \frac{r}{k}\right).$$

Si $m = 1, 2, 3, \dots$ utilizamos (32) para obtener

$$|L(s, \chi)| \leq k^{-\sigma} \sum_{r=1}^{k-1} \left| \zeta\left(s, \frac{r}{k}\right) \right| < k^{m+\delta} k A(\delta) |t|^{m+1+\delta}$$

que prueba (33) para $m \geq 1$. Si $m = 0$ ó -1 escribimos

$$(34) \quad L(s, \chi) = \sum_{r=1}^{k-1} \frac{\chi(r)}{r^s} + k^{-s} \sum_{r=1}^{k-1} \chi(r) \left\{ \zeta\left(s, \frac{r}{k}\right) - \left(\frac{r}{k}\right)^{-s} \right\}.$$

Como $-m - \delta \leq \sigma \leq -m + \delta$ podemos utilizar (30) y (31) para obtener

$$k^{-\sigma} \left| \zeta\left(s, \frac{r}{k}\right) - \left(\frac{r}{k}\right)^{-s} \right| \leq k^{m+\delta} A(\delta) |t|^{m+1+\delta},$$

luego la segunda suma de (34) se halla dominada por $A(\delta) |kt|^{m+1+\delta}$. La primera suma está dominada por

$$\sum_{r=1}^{k-1} \frac{1}{r^\sigma} \leq \sum_{r=1}^{k-1} r^{m+\delta} < 1 + \int_1^k x^{m+\delta} dx = \frac{k^{m+1+\delta}}{m+1+\delta} \leq \frac{k^{m+1+\delta}}{\delta},$$

y esta suma queda absorbida en la acotación $A(\delta) |kt|^{m+1+\delta}$. □

Ejercicios del capítulo 12

1. Sea $f(n)$ una función aritmética periódica módulo k .

(a) Probar que la serie de Dirichlet $\sum f(n)n^{-s}$ converge absolutamente para $\sigma > 1$ y que

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = k^{-s} \sum_{r=1}^k f(r) \zeta\left(s, \frac{r}{k}\right) \quad \text{si } \sigma > 1.$$

(b) Si $\sum_{r=1}^k f(r) = 0$ probar que la serie de Dirichlet $\sum f(n)n^{-s}$ converge para $\sigma < 0$ y que existe una función entera $F(s)$ tal que $F(s) = \sum f(n)n^{-s}$ para $\sigma > 0$.

2. Si x es real y $\sigma > 1$, sea $F(x, s)$ la función zeta periódica

$$F(x, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s}.$$

Si $0 < a < 1$ y $\sigma > 1$ probar que la fórmula de Hurwitz implica

$$F(a, s) = \frac{\Gamma(1-s)}{(2\pi)^{1-s}} \{e^{\pi i(1-s)/2} \zeta(1-s, a) + e^{\pi i(s-1)/2} \zeta(1-s, 1-a)\}.$$

3. La fórmula del ejercicio 2 se puede utilizar para extender la definición de $F(a, s)$ sobre el s -plano entero si $0 < a < 1$. Probar que $F(a, s)$, extendida de esta forma, es una función entera de s .
4. Si $0 < a < 1$ y $0 < b < 1$, sea

$$\Phi(a, b, s) = \frac{\Gamma(s)}{(2\pi)^s} \{\zeta(s, a)F(b, 1+s) + \zeta(s, 1-a)F(1-b, 1+s)\},$$

en donde F es la función del ejercicio 2. Probar que

$$\begin{aligned} \frac{\Phi(a, b, s)}{\Gamma(s)\Gamma(-s)} &= e^{\pi i s/2} \{\zeta(s, a)\zeta(-s, 1-b) + \zeta(s, 1-a)\zeta(-s, b)\} \\ &\quad + e^{-\pi i s/2} \{\zeta(-s, 1-b)\zeta(s, 1-a) + \zeta(-s, b)\zeta(s, a)\}, \end{aligned}$$

y deducir que $\Phi(a, b, s) = \Phi(1-b, a, -s)$. Esta ecuación funcional es útil en la teoría de las funciones elípticas modulares.

En los ejercicios 5, 6 y 7, $\xi(s)$ designa la función entera introducida en la sección 12.8,

$$\xi(s) = \frac{1}{2} s(s-1) \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

5. Probar que $\xi(s)$ es real sobre las rectas $t=0$ y $\sigma=1/2$, y que $\xi(0) = \xi(1) = 1/2$.
6. Probar que los ceros de $\xi(s)$ (si existen) se hallan todos ellos situados en la banda $0 \leq \sigma \leq 1$ y su colocación es simétrica respecto de las rectas $t=0$ y $\sigma=1/2$.
7. Probar que los ceros de $\zeta(s)$ en la banda crítica $0 < \sigma < 1$ (si existen) son idénticos en posición y en orden de multiplicidad que los de $\xi(s)$.
8. Sea χ un carácter primitivo mod k . Definimos

$$a = a(\chi) = \begin{cases} 0 & \text{si } \chi(-1) = 1, \\ 1 & \text{si } \chi(-1) = -1. \end{cases}$$

(a) Probar que la ecuación funcional de $L(s, \chi)$ tiene la forma

$$L(1-s, \bar{\chi}) = a(\chi) 2(2\pi)^{-s} k^{s-1/2} \cos\left(\frac{\pi(s-a)}{2}\right) \Gamma(s) L(s, \chi), \text{ donde } |a(\chi)| = 1.$$

(b) Sea

$$\xi(s, \chi) = \left(\frac{k}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s, \chi).$$

Probar que $\xi(1-s, \bar{\chi}) = \varepsilon(\chi) \xi(s, \chi)$.

9. Referente al ejercicio 8.

(a) Probar que $\xi(s, \chi) \neq 0$ si $\sigma > 1$ o $\sigma < 0$.

(b) Describir la colocación de los ceros de $L(s, \chi)$ en el semiplano $\sigma < 0$.

10. Sea χ un carácter no primitivo mod k . Describir la colocación de los ceros de $L(s, \chi)$ en el semiplano $\sigma < 0$.

11. Probar que los polinomios de Bernoulli satisfacen las relaciones

$$B_n(1-x) = (-1)^n B_n(x) \quad \text{y} \quad B_{2n+1}(\tfrac{1}{2}) = 0 \quad \text{para todo } n \geq 0.$$

12. B_n designa el n -ésimo número de Bernoulli. Obsérvese que

$$\begin{aligned} B_2 &= \tfrac{1}{6} = 1 - \tfrac{1}{2} - \tfrac{1}{3}, & B_4 &= -\tfrac{1}{30} = 1 - \tfrac{1}{2} - \tfrac{1}{3} - \tfrac{1}{5}, \\ B_6 &= \tfrac{1}{42} = 1 - \tfrac{1}{2} - \tfrac{1}{3} - \tfrac{1}{7}. \end{aligned}$$

Estas fórmulas ilustran un teorema descubierto en 1840 por von Staudt y Clausen (independientemente). Si $n \geq 1$ tenemos

$$B_{2n} = I_n - \sum_{p-1|2n} \frac{1}{p},$$

en donde I_n es un entero y la suma se halla extendida a todos los primos p tales que $p-1$ divide a $2n$. Este ejercicio esboza una demostración que se debe a Lucas.

(a) Probar que

$$B_n = \sum_{k=0}^n \frac{1}{k+1} \sum_{r=0}^k (-1)^r \binom{k}{r} r^n.$$

[Indicación: Escribir $x = \log \{1 + (e^x - 1)\}$ y utilizar las series de potencias para $x/(e^x - 1)$.]

(b) Probar que

$$B_n = \sum_{k=0}^n \frac{k!}{k+1} c(n, k),$$

en donde $c(n, k)$ es un entero.

(c) Si a y b son enteros con $a \geq 2$, $b \geq 2$ y $ab > 4$, probar que $ab|(ab-1)!$. Este hecho demuestra que en la suma de la parte (b), cada término con $k+1$ compuesto, $k > 3$, es un entero.

(d) Si p es primo, probar que

$$\sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} r^n \equiv \begin{cases} -1 \pmod{p} & \text{si } p-1|n, n > 0, \\ 0 \pmod{p} & \text{si } p-1 \nmid n. \end{cases}$$

(e) Utilizar los resultados anteriores o algún otro medio para probar el teorema de von Staudt-Clausen.

13. Probar que la derivada del polinomio de Bernoulli $B_n(x)$ es $nB_{n-1}(x)$ si $n \geq 2$.

14. Probar que los polinomios de Bernoulli satisfacen la fórmula aditiva

$$B_n(x+y) = \sum_{k=0}^n \binom{n}{k} B_k(x) y^{n-k}.$$

15. Probar que los polinomios de Bernoulli satisfacen la fórmula multiplicativa

$$B_p(mx) = m^{p-1} \sum_{k=0}^{m-1} B_p\left(x + \frac{k}{m}\right).$$

16. Probar que, si $r \geq 1$, los números de Bernoulli satisfacen la relación

$$\sum_{k=0}^r \frac{2^{2k} B_{2k}}{(2k)!(2r+1-2k)!} = \frac{1}{(2r)!}.$$

17. Calcular la integral $\int_0^1 x B_p(x) dx$ de dos formas distintas y deducir la fórmula

$$\sum_{r=0}^p \binom{p}{r} \frac{B_r}{p+2-r} = \frac{B_{p+1}}{p+1}.$$

18. (a) Comprobar la identidad

$$\begin{aligned} \frac{uv}{(e^u-1)(e^v-1)} \frac{e^{u+v}-1}{u+v} &= \frac{uv}{u+v} \left(1 + \frac{1}{e^u-1} + \frac{1}{e^v-1}\right) \\ &= 1 + \sum_{n=2}^{\infty} \frac{uv}{n!} \left(\frac{u^{n-1} + v^{n-1}}{u+v}\right) B_n. \end{aligned}$$

(b) Sea $J = \int_0^1 B_p(x) B_q(x) dx$. Probar que J es el coeficiente de $p!q!u^p v^q$ en el desarrollo de la parte (a). Utilizarlo para deducir que

$$\int_0^1 B_p(x) B_q(x) dx = \begin{cases} (-1)^{p+1} \frac{p!q!}{(p+q)!} B_{p+q} & \text{si } p \geq 1, q \geq 1, \\ 1 & \text{si } p = q = 0, \\ 0 & \text{si } p \geq 1, q = 0; \text{ o } p = 0, q \geq 1. \end{cases}$$

19. (a) Utilizar un método análogo al del ejercicio 18 para obtener la identidad

$$(u+v) \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} B_m(x) B_n(x) \frac{u^m v^n}{m!n!} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} B_{m+n}(x) \frac{u^m v^n}{m!n!} \sum_{r=0}^{\infty} \frac{B_{2r}}{(2r)!} (u^{2r} v + uv^{2r}).$$

(b) Comparar los coeficientes de (a) e integrar el resultado para obtener la fórmula

$$B_m(x)B_n(x) = \sum_r \left\{ \binom{m}{2r}n + \binom{n}{2r}m \right\} \frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r} + (-1)^{m+1} \frac{m!n!}{(m+n)!} B_{m+n}$$

para $m \geq 1$, $n \geq 1$. Indicar el recorrido del índice r .

20. Probar que, si $m \geq 1$, $n \geq 1$, y $p \geq 1$, tenemos

$$\begin{aligned} \int_0^1 B_m(x)B_n(x)B_p(x) dx \\ = (-1)^{p+1} p! \sum_r \left\{ \binom{m}{2r}n + \binom{n}{2r}m \right\} \frac{(m+n-2r-1)!}{(m+n+p-2r)!} B_{2r}B_{m+n+p-2r}. \end{aligned}$$

En particular, calcular $\int_0^1 B_2^3(x) dx$ a partir de esta fórmula.

21. Sea $f(n)$ una función aritmética periódica mod k , y sea

$$g(n) = \frac{1}{k} \sum_{m \bmod k} f(m) e^{-2\pi i m n / k}$$

la sucesión finita de coeficientes de Fourier de f . Si

$$F(s) = k^{-s} \sum_{r=1}^k f(r) \zeta\left(s, \frac{r}{k}\right),$$

probar que

$$F(1-s) = \frac{\Gamma(s)}{(2\pi)^s} \left\{ e^{\pi i s/2} \sum_{r=1}^k g(r) \zeta\left(s, \frac{r}{k}\right) + e^{-\pi i s/2} \sum_{r=1}^k g(-r) \zeta\left(s, \frac{r}{k}\right) \right\}.$$

22. Sea χ un carácter no principal mod k y sea $S(x) = \sum_{n \leq x} \chi(n)$.

(a) Si $N \geq 1$ y $\sigma > 0$ probar que

$$L(s, \chi) = \sum_{n=1}^N \frac{\chi(n)}{n^s} + s \int_N^\infty \frac{S(x) - S(N)}{x^{s+1}} dx.$$

(b) Si $s = \sigma + it$ con $\sigma \geq \delta > 0$ y $|t| \geq 0$, utilizar la parte (a) para probar que existe una constante $A(\delta)$ tal que

$$|L(s, \chi)| \leq A(\delta) B(k) (|t| + 1)^{1-\delta}$$

en donde $B(k)$ es una cota superior de $|S(x)|$. En el teorema 13.15 se demuestra que $B(k) = O(\sqrt{k} \log k)$.

(c) Probar que, para cierta constante $A > 0$, tenemos

$$|L(s, \chi)| \leq A \log k \quad \text{si } \sigma \geq 1 - \frac{1}{\log k} \quad \text{y } 0 \leq |t| \leq 2.$$

[Indicación: Hacer $N = k$ en la parte (a).]

Capítulo 13

Demostración analítica del teorema del número primo

13.1 EL PLAN DE LA DEMOSTRACIÓN

El teorema del número primo es equivalente a la afirmación

$$(1) \quad \psi(x) \sim x \quad \text{cuando } x \rightarrow \infty,$$

en donde $\psi(x)$ es la función de Chebyshev,

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Este capítulo proporciona una demostración analítica de (1) basada en las propiedades de la función zeta de Riemann. La demostración analítica es más breve que la demostración elemental efectuada en el capítulo 4 y sus ideas principales se comprenden con mayor facilidad. Esta sección describe los hechos más sobresalientes de la demostración.

La función ψ es una función escalonada y resulta más conveniente tratar con su integral que designamos ψ_1 . Por lo tanto, sea

$$\psi_1(x) = \int_1^x \psi(t) dt.$$

La integral ψ_1 es una función continua lineal a trozos. Ante todo veremos que la relación asintótica

$$(2) \quad \psi_1(x) \sim \frac{1}{2} x^2 \quad \text{cuando } x \rightarrow \infty$$

implica (1) y por tanto demuestra (2). A este fin expresamos $\psi_1(x)/x^2$ en términos de la función zeta de Riemann mediante la integral de contorno,

$$\frac{\psi_1(x)}{x^2} = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) ds, \quad \text{en donde } c > 1.$$

El cociente $-\zeta'(s)/\zeta(s)$ posee un polo de primer orden en $s = -1$ con residuo 1. Si quitamos este polo obtenemos la fórmula

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x} \right)^2 = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} \right) ds, \quad \text{para } c > 1.$$

Sea

$$h(s) = \frac{1}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} \right)$$

y escribamos de nuevo la última ecuación en la forma

$$(3) \quad \begin{aligned} \frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x} \right)^2 &= \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} x^{s-1} h(s) ds \\ &= \frac{x^{c-1}}{2\pi} \int_{-\infty}^{+\infty} h(c+it) e^{it \log x} dt. \end{aligned}$$

Para completar la demostración debemos probar que

$$(4) \quad \lim_{x \rightarrow \infty} \frac{x^{c-1}}{2\pi} \int_{-\infty}^{+\infty} h(c+it) e^{it \log x} dt = 0.$$

Entonces el lema de Riemann-Lebesgue de la teoría de las series de Fourier establece que

$$\lim_{x \rightarrow \infty} \int_{-\infty}^{+\infty} f(t) e^{itx} dt = 0$$

si la integral $\int_{-\infty}^{+\infty} |f(t)| dt$ converge. La integral en (4) es de este tipo con $\log x$ reemplazando a x , y es fácil demostrar que la integral $\int_{-\infty}^{+\infty} |h(c + it)| dt$ converge si $c > 1$, por lo que la integral de (4) tiende a 0 cuando $x \rightarrow \infty$. Sin embargo, el factor x^{c-1} que se halla fuera de la integral tiende a ∞ cuando $c > 1$, por lo que nos enfrentamos con una indeterminación del tipo $\infty \cdot 0$. La ecuación (3) se verifica para todo $c > 1$. Si hacemos $c = 1$ en (3) el factor inoportuno x^{c-1} desaparece. Pero entonces $h(c + it)$ se transforma en $h(1 + it)$ y el integrando contiene a $\zeta'(s)/\zeta(s)$ sobre la recta $\sigma = 1$. En este caso resulta más difícil demostrar que la integral $\int_{-\infty}^{+\infty} |h(1 + it)| dt$ converge, y este hecho debe ser demostrado antes de poder aplicar el lema de Riemann-Lebesgue. La última y más difícil parte de la demostración consiste en demostrar que es posible substituir c por 1 en (3) y que la integral $\int_{-\infty}^{+\infty} |h(1 + it)| dt$ converge. Requiere un estudio más detallado de la función zeta de Riemann en las proximidades de la recta $\sigma = 1$.

Ahora procederemos a llevar a término el plan ahora esbozado. Empezaremos con unos lemas.

13.2 LEMAS

Lema 1 Para toda función aritmética $a(n)$, sea

$$A(x) = \sum_{n \leq x} a(n),$$

en donde $A(x) = 0$ si $x < 1$. Entonces

$$(5) \quad \sum_{n \leq x} (x - n)a(n) = \int_1^x A(t) dt.$$

DEMOSTRACIÓN. Aplicamos la identidad de Abel (teorema 4.2) que establece que

$$(6) \quad \sum_{n \leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t) dt$$

si f posee derivada continua en $[1, x]$. Hacemos $f(t) = t$ y obtenemos

$$\sum_{n \leq x} a(n)f(n) = \sum_{n \leq x} na(n) \quad \text{y} \quad A(x)f(x) = x \sum_{n \leq x} a(n)$$

por lo que (6) reduce a (5). $\square$

El lema que sigue constituye una forma de la regla de l'Hôpital para funciones crecientes lineales a trozos.

Lema 2 Sea $A(x) = \sum_{n \leq x} a(n)$ y sea $A_1(x) = \int_1^x A(t) dt$. Además suponemos que $a(n) \geq 0$ para todo n . Si tenemos la fórmula asintótica

$$(7) \quad A_1(x) \sim Lx^c \quad \text{cuando } x \rightarrow \infty$$

para un $c > 0$ y un $L > 0$, entonces también tenemos

$$(8) \quad A(x) \sim cLx^{c-1} \quad \text{cuando } x \rightarrow \infty.$$

Con otras palabras, la diferenciación formal de (7) nos proporciona un resultado correcto.

DEMOSTRACIÓN. La función $A(x)$ es creciente puesto que los $a(n)$ son no negativos. Elegimos un $\beta > 1$ y consideramos la diferencia $A_1(\beta x) - A_1(x)$. Tenemos

$$\begin{aligned} A_1(\beta x) - A_1(x) &= \int_x^{\beta x} A(u) du \geq \int_x^{\beta x} A(x) du = A(x)(\beta x - x) \\ &= x(\beta - 1)A(x). \end{aligned}$$

Esto nos da

$$xA(x) \leq \frac{1}{\beta - 1} \{A_1(\beta x) - A_1(x)\}$$

luego

$$\frac{A(x)}{x^{c-1}} \leq \frac{1}{\beta - 1} \left\{ \frac{A_1(\beta x)}{(\beta x)^c} \beta^c - \frac{A_1(x)}{x^c} \right\}.$$

Fijamos β y hacemos que $x \rightarrow \infty$ en la desigualdad anterior. Obtenemos

$$\limsup_{x \rightarrow \infty} \frac{A(x)}{x^{c-1}} \leq \frac{1}{\beta - 1} (L\beta^c - L) = L \frac{\beta^c - 1}{\beta - 1}.$$

Ahora hacemos que $\beta \rightarrow 1 +$. El cociente de la derecha es el cociente incremental relativo a la derivada de x^c en $x = 1$ y tiene límite c . Por consiguiente

$$(9) \quad \limsup_{x \rightarrow \infty} \frac{A(x)}{x^{c-1}} \leq cL.$$

Ahora consideramos un α con $0 < \alpha < 1$ y consideramos la diferencia $A_1(x) - A_1(\alpha x)$. Un razonamiento análogo al anterior demuestra que

$$\liminf_{x \rightarrow \infty} \frac{A(x)}{x^{c-1}} \geq L \frac{1 - \alpha^c}{1 - \alpha}.$$

Cuando $\alpha \rightarrow 1$ — el segundo miembro tiende a cL . Esto, junto con (9), prueba que $A(x)/x^{c-1}$ tiende al límite cL cuando $x \rightarrow \infty$. $\square$

Cuando $a(n) = \Lambda(n)$ tenemos $A(x) = \psi(x)$, $A_1(x) = \psi_1(x)$, y $a(n) \geq 0$. Por consiguiente podemos aplicar los lemas 1 y 2 y obtenemos inmediatamente:

Teorema 13.1 *Tenemos*

$$(10) \quad \psi_1(x) = \sum_{n \leq x} (x - n) \Lambda(n).$$

Además, la relación asintótica $\psi_1(x) \sim x^2/2$ implica $\psi(x) \sim x$ cuando $x \rightarrow \infty$.

Nuestra próxima labor consiste en expresar $\psi_1(x)/x^2$ como una integral de contorno que involucre a la función zeta. Para ello precisamos de los casos especiales $k = 1$ y $k = 2$ del siguiente lema sobre integrales de contorno. (Compárese con el lema 4 del capítulo 11.)

Lema 3 *Si $c > 0$ y $u > 0$, entonces para cada entero $k \geq 1$ tenemos*

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{u^{-z}}{z(z+1) \cdots (z+k)} dz = \begin{cases} \frac{1}{k!} (1-u)^k & \text{si } 0 < u \leq 1, \\ 0 & \text{si } u > 1, \end{cases}$$

y la integral es absolutamente convergente.

DEMOSTRACIÓN. En primer lugar observamos que el integrando es igual a $u^{-z} \Gamma(z)/\Gamma(z+k+1)$. Este resultado se obtiene utilizando repetidamente la ecuación funcional $\Gamma(z+1) = z\Gamma(z)$. Para probar el lema aplicamos el teorema del residuo de Cauchy a la integral

$$\frac{1}{2\pi i} \int_{C(R)} \frac{u^{-z} \Gamma(z)}{\Gamma(z+k+1)} dz,$$

en donde $C(R)$ es el contorno dibujado en la figura 13.1(a) si $0 < u \leq 1$, y el de la figura 13.1(b) si $u > 1$. El radio R del círculo es mayor que $2k+c$ por lo que todos los polos en $z=0, -1, \dots, -k$ se hallan en el interior del círculo.

Ahora vemos que el integrando a lo largo de cada uno de los arcos circulares tiende a 0 cuando $R \rightarrow \infty$. Si $z = x + iy$ y $|z| = R$, el integrando se halla dominado por

$$\left| \frac{u^{-z}}{z(z+1)\cdots(z+k)} \right| = \frac{u^{-x}}{|z||z+1|\cdots|z+k|} \leq \frac{u^{-c}}{R|z+1|\cdots|z+k|}.$$

La desigualdad $u^{-x} \leq u^{-c}$ se sigue del hecho de que u^{-x} es una función creciente de x si $0 < u \leq 1$ y decreciente si $u > 1$. Ahora, si $1 \leq n \leq k$, tenemos

$$|z+n| \geq |z| - n = R - n \geq R - k \geq R/2$$

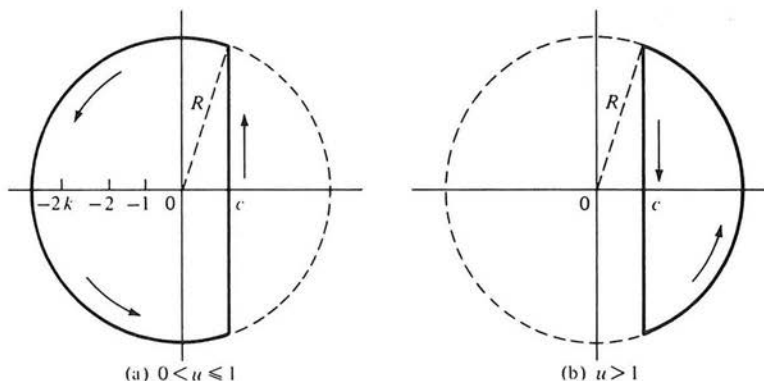


Figura 13.1

puesto que $R > 2k$. Por consiguiente la integral a lo largo de cada arco circular se halla acotada por

$$\frac{2\pi R u^{-c}}{R(\frac{1}{2}R)^k} = O(R^{-k})$$

y ésta $\rightarrow 0$ cuando $R \rightarrow \infty$ ya que $k \geq 1$.

Si $u > 1$, el integrando es analítico en el interior de $C(R)$, luego $\int_{C(R)} = 0$. Si ahora $R \rightarrow \infty$ el lema queda establecido en este caso.

Si $0 < u \leq 1$, calculamos la integral a lo largo de $C(R)$ por el teorema del residuo de Cauchy. El integrando posee polos en los puntos enteros $n = 0, -1, \dots, -k$, luego

$$\begin{aligned} \frac{1}{2\pi i} \int_{C(R)} \frac{u^{-z} \Gamma(z)}{\Gamma(z+k+1)} dz &= \sum_{n=0}^k \operatorname{Res}_{z=-n} \frac{u^{-z} \Gamma(z)}{\Gamma(z+k+1)} \\ &= \sum_{n=0}^k \frac{u^n}{\Gamma(k+1-n)} \operatorname{Res}_{z=-n} \Gamma(z) = \sum_{n=0}^k \frac{u^n (-1)^n}{(k-n)! n!} \\ &= \frac{1}{k!} \sum_{n=0}^k \binom{k}{n} (-u)^n = \frac{(1-u)^k}{k!}. \end{aligned}$$

Si $R \rightarrow \infty$ obtenemos el lema. □

13.3 UNA REPRESENTACIÓN DE $\psi_1(x)/x^2$ COMO INTEGRAL DE CONTORNO

Teorema 13.2 Si $c > 1$ y $x \geq 1$ tenemos

$$(11) \quad \frac{\psi_1(x)}{x^2} = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^{s-1}}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) ds.$$

DEMOSTRACIÓN. De la ecuación (10) tenemos $\psi_1(x)/x = \sum_{n \leq x} (1 - n/x) \Lambda(n)$. Ahora usamos el lema 3 con $k = 1$ y $u = n/x$. Si $n \leq x$ obtenemos

$$1 - \frac{n}{x} = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{(x/n)^s}{s(s+1)} ds.$$

Multiplicamos esta relación por $\Lambda(n)$ y sumamos para todos los $n \leq x$ y obtenemos

$$\frac{\psi_1(x)}{x} = \sum_{n \leq x} \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{\Lambda(n)(x/n)^s}{s(s+1)} ds = \sum_{n=1}^{\infty} \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{\Lambda(n)(x/n)^s}{s(s+1)} ds$$

ya que la integral se anula si $n > x$. Podemos escribirla

$$(12) \quad \frac{\psi_1(x)}{x} = \sum_{n=1}^{\infty} \int_{c-\infty i}^{c+\infty i} f_n(s) ds,$$

en donde $2\pi i f_n(s) = \Lambda(n) (x/n)^s / (s^2 + s)$. Ahora, en (12), queremos intercambiar la suma y la integral. Para ello es suficiente probar que la serie

$$(13) \quad \sum_{n=1}^{\infty} \int_{c-\infty i}^{c+\infty i} |f_n(s)| ds$$

es convergente. (Ver teorema 10.26 de [2].) Las sumas parciales de esta serie satisfacen la desigualdad

$$\sum_{n=1}^N \int_{c-\infty i}^{c+\infty i} \frac{\Lambda(n)(x/n)^c}{|s||s+1|} ds = \sum_{n=1}^N \frac{\Lambda(n)}{n^c} \int_{c-\infty i}^{c+\infty i} \frac{x^c}{|s||s+1|} ds \leq A \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^c},$$

en donde A es constante, luego (13) converge. Por tanto podemos intercambiar la suma y la integral en (12) y obtenemos

$$\begin{aligned} \frac{\psi_1(x)}{x} &= \int_{c-\infty i}^{c+\infty i} \sum_{n=1}^{\infty} f_n(s) ds = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} ds \\ &= \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) ds. \end{aligned}$$

Ahora, para obtener (11), basta dividir por x . □

Teorema 13.3 Si $c > 1$ y $x \geq 1$ tenemos

$$(14) \quad \frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} x^{s-1} h(s) ds,$$

en donde

$$(15) \quad h(s) = \frac{1}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} \right).$$

DEMOSTRACIÓN. Esta vez utilizaremos el lema 3 con $k=2$ para obtener

$$\frac{1}{2} \left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \frac{x^s}{s(s+1)(s+2)} ds,$$

en donde $c > 0$. Substituimos s por $s-1$ en la integral (haciendo $c > 1$) y restamos este resultado de (11) para obtener el teorema 13.3. $\square$

Si parametrizamos el arco de integración haciendo $s = c + it$, obtenemos $x^{s-1} = x^{c-1} x^{it} = x^{c-1} e^{it \log x}$ y la ecuación (14) se transforma en

$$(16) \quad \frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x}\right)^2 = \frac{x^{c-1}}{2} \int_{c-\infty i}^{c+\infty i} h(c+it) e^{it \log x} dt.$$

Nuestra próxima labor consiste en demostrar que el segundo miembro de (16) tiende a 0 cuando $x \rightarrow \infty$. Como ya hemos indicado anteriormente, primero probaremos que podemos hacer $c=1$ en (16). A este fin necesitamos estudiar $\zeta(s)$ en las proximidades de la recta $\sigma=1$.

13.4 COTAS SUPERIORES PARA $|\zeta(s)|$ Y PARA $|\zeta'(s)|$ EN LAS PROXIMIDADES DE LA RECTA $\sigma=1$

Para estudiar $\zeta(s)$ en las proximidades de la recta $\sigma=1$ utilizamos la representación que se obtiene por el teorema 12.21 y que es válida para $\sigma > 0$,

$$(17) \quad \zeta(s) = \sum_{n=1}^N \frac{1}{n^s} - s \int_N^{\infty} \frac{x - [x]}{x^{s+1}} dx + \frac{N^{1-s}}{s-1}.$$

Utilizamos además la fórmula correspondiente a $\zeta'(s)$ que se obtiene derivando cada uno de los miembros de (17),

$$(18) \quad \zeta'(s) = - \sum_{n=1}^N \frac{\log n}{n^s} + s \int_N^{\infty} \frac{(x - [x]) \log x}{x^{s+1}} dx - \int_N^{\infty} \frac{x - [x]}{x^{s+1}} dx \\ - \frac{N^{1-s} \log N}{s-1} - \frac{N^{1-s}}{(s-1)^2}.$$

El teorema que sigue utiliza estas relaciones para obtener cotas superiores de $|\zeta(s)|$ y de $|\zeta'(s)|$.

Teorema 13.4 Para cada $A > 0$, existe una constante M (que depende de A) tal que

$$(19) \quad |\zeta(s)| \leq M \log t \quad y \quad |\zeta'(s)| \leq M \log^2 t$$

para todo s con $\sigma \geq 1/2$ que además verifica

$$(20) \quad \sigma > 1 - \frac{A}{\log t} \quad y \quad t \geq e.$$

Nota. Las desigualdades de (20) describen una región del tipo representado en la figura 13.2.

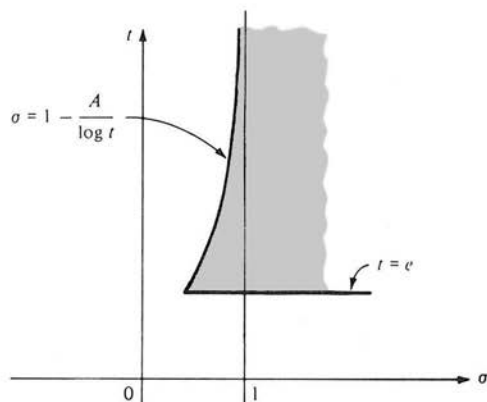


Figura 13.2

DEMOSTRACIÓN. Si $\sigma \geq 2$, tenemos $|\zeta(s)| \leq \zeta(2)$ y $|\zeta'(s)| \leq |\zeta'(2)|$ y las desigualdades de (19) se verifican trivialmente. Por consiguiente podemos suponer que $\sigma < 2$ y $t \geq e$. Entonces tenemos

$$|s| \leq \sigma + t \leq 2 \leq t < 2t \quad \text{y} \quad |s - 1| \geq t$$

luego $1/|s| \leq 1/t$. Si acotamos $|\zeta(s)|$ utilizando (17) obtenemos

$$|\zeta(s)| \leq \sum_{n=1}^N \frac{1}{n^\sigma} + 2t \int_N^\infty \frac{1}{x^{\sigma+1}} dx + \frac{N^{1-\sigma}}{t} = \sum_{n=1}^N \frac{1}{n^\sigma} + \frac{2t}{\sigma N^\sigma} + \frac{N^{1-\sigma}}{t}.$$

Ahora hacemos que N dependa de t tomando $N = [t]$. Entonces $N \leq t < N + 1$ y $\log n \leq \log t$ si $n \leq N$. La desigualdad de (20) implica $1 - \sigma < A/\log t$ por lo tanto

$$\frac{1}{n^\sigma} = \frac{n^{1-\sigma}}{n} = \frac{1}{n} e^{(1-\sigma) \log n} < \frac{1}{n} e^{A \log n / \log t} \leq \frac{1}{n} e^A = O\left(\frac{1}{n}\right).$$

Por consiguiente

$$\frac{2t}{\sigma N^\sigma} \leq \frac{N+1}{N} = O(1) \quad \text{y} \quad \frac{N^{1-\sigma}}{t} = \frac{N}{t} \frac{1}{N^\sigma} = O\left(\frac{1}{N}\right) = O(1),$$

luego

$$|\zeta(s)| = O\left(\sum_{n=1}^N \frac{1}{n}\right) + O(1) = O(\log N) + O(1) = O(\log t).$$

Esto demuestra la desigualdad relativa a $|\zeta(s)|$ dada en (19). Para obtener la desigualdad relativa a $|\zeta'(s)|$ aplicamos el mismo tipo de razonamiento a (18). La única diferencia esencial es que en el miembro de la derecha aparece el factor extra $\log N$. Pero $\log N = O(\log t)$ por lo que en la región especificada tenemos $|\zeta'(s)| = O(\log^2 t)$. $\square$

13.5 LA NO ANULACIÓN DE $\zeta(s)$ EN LA RECTA $\sigma = 1$

En esta sección vemos que $\zeta(1 + it) \neq 0$ para cada t real. La demostración se basa en una desigualdad que también necesitaremos en la sección siguiente.

Teorema 13.5 Si $\sigma > 1$ tenemos

$$(21) \quad \zeta^3(\sigma) |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \geq 1.$$

DEMOSTRACIÓN. Recordamos la identidad $\zeta(s) = e^{G(s)}$ demostrada en la sección 11.9, ejemplo 1, en donde

$$G(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s} = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} \quad (\sigma > 1)$$

se puede escribir

$$\zeta(s) = \exp \left\{ \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} \right\} = \exp \left\{ \sum_p \sum_{m=1}^{\infty} \frac{e^{-imt \log p}}{mp^{m\sigma}} \right\},$$

de donde obtenemos

$$|\zeta(s)| = \exp \left\{ \sum_p \sum_{m=1}^{\infty} \frac{\cos(mt \log p)}{mp^{m\sigma}} \right\}.$$

Aplicamos esta fórmula repetidamente con $s = \sigma$, $s = \sigma + it$ y $s = \sigma + 2it$, y se obtiene

$$\begin{aligned} & \zeta^3(\sigma) |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \\ &= \exp \left\{ \sum_p \sum_{m=1}^{\infty} \frac{3 + 4 \cos(mt \log p) + \cos(2mt \log p)}{mp^{m\sigma}} \right\}. \end{aligned}$$

Ahora bien, disponemos de la desigualdad trigonométrica

$$3 + 4 \cos \theta + \cos 2\theta \geq 0$$

que se obtiene a partir de la identidad

$$3 + 4 \cos \theta + \cos 2\theta = 3 + 4 \cos \theta + 2 \cos^2 \theta - 1 = 2(1 + \cos \theta)^2.$$

Por consiguiente cada término de la última serie infinita es no negativo y obtenemos (21). $\square$

Teorema 13.6 *Tenemos $\zeta(1 + it) \neq 0$ para cada t real.*

DEMOSTRACIÓN. Únicamente debemos considerar $t \neq 0$. Se puede escribir (21) en la forma

$$(22) \quad \{(\sigma - 1)\zeta(\sigma)\}^3 \left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1}.$$

Esto es válido si $\sigma > 1$. Ahora hacemos que $\sigma \rightarrow 1 +$ en (22). El primer factor tiende a 1 puesto que $\zeta(s)$ tiene residuo 1 en el polo $s = 1$. El tercer factor tiende a $|\zeta(1 + 2it)|$. Si $\zeta(1 + it)$ fuese cero, el segundo factor podríamos escribirlo

$$\left| \frac{\zeta(\sigma + it) - \zeta(1 + it)}{\sigma - 1} \right|^4 \rightarrow |\zeta'(1 + it)|^4 \quad \text{cuando } \sigma \rightarrow 1 +.$$

Por consiguiente, si para algún $t \neq 0$ tuviésemos $\zeta(1 + it) = 0$, el primer miembro de (22) se aproximaría al límite $|\zeta'(1 + it)|^4 |\zeta(1 + 2it)|$ cuando $\sigma \rightarrow 1 +$. Pero el segundo miembro tiende a ∞ cuando $\sigma \rightarrow 1 +$ y ello no es posible. $\square$

13.6 DESIGUALDADES PARA $|1/\zeta(s)|$ Y $|\zeta'(s)/\zeta(s)|$

Aplicamos ahora una vez más el teorema 13.5 y obtenemos las siguientes desigualdades para $|1/\zeta(s)|$ y $|\zeta'(s)/\zeta(s)|$.

Teorema 13.7 *Existe una constante $M > 0$ tal que*

$$\left| \frac{1}{\zeta(s)} \right| < M \log^7 t \quad y \quad \left| \frac{\zeta'(s)}{\zeta(s)} \right| < M \log^9 t$$

si $\sigma \geq 1$ y $t \geq e$.

DEMOSTRACIÓN. Para $\sigma \geq 2$ tenemos

$$\left| \frac{1}{\zeta(s)} \right| = \left| \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^2} \leq \zeta(2)$$

y

$$\left| \frac{\zeta'(s)}{\zeta(s)} \right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^2},$$

luego las desigualdades se verifican trivialmente si $\sigma \geq 2$. Suponemos, entonces, que $1 \leq \sigma \leq 2$ y que $t \geq e$. Escribimos de nuevo las desigualdades de (21) como sigue:

$$\frac{1}{|\zeta(\sigma + it)|} \leq \zeta(\sigma)^{3/4} |\zeta(\sigma + 2it)|^{1/4}.$$

Ahora, como $(\sigma - 1)\zeta(\sigma)$ está acotado en el intervalo $1 \leq \sigma \leq 2$, o sea que $(\sigma - 1)\zeta(\sigma) \leq M$, en donde M es una constante, tenemos

$$\zeta(\sigma) \leq \frac{M}{\sigma - 1} \quad \text{si } 1 < \sigma \leq 2.$$

Además, $\zeta(\sigma + 2it) = O(\log t)$ si $1 \leq \sigma \leq 2$ (por el teorema 13.4), luego para $1 < \sigma \leq 2$ tenemos

$$\frac{1}{|\zeta(\sigma + it)|} \leq \frac{M^{3/4}(\log t)^{1/4}}{(\sigma - 1)^{3/4}} = \frac{A(\log t)^{1/4}}{(\sigma - 1)^{3/4}},$$

en donde A es una constante absoluta. Por consiguiente, para una constante $B > 0$, tenemos

$$(23) \quad |\zeta(\sigma + it)| > \frac{B(\sigma - 1)^{3/4}}{(\log t)^{1/4}}, \quad \text{si } 1 < \sigma \leq 2, \text{ y } t \geq e.$$

Esto también se verifica trivialmente para $\sigma = 1$. Sea α un número cualquiera que verifique $1 < \alpha < 2$. Entonces, si $1 \leq \sigma \leq \alpha$, $t \geq e$, podemos utilizar el teorema 13.4 para escribir

$$\begin{aligned} |\zeta(\sigma + it) - \zeta(\alpha + it)| &\leq \int_{\sigma}^{\alpha} |\zeta'(u + it)| du \leq (\alpha - \sigma)M \log^2 t \\ &\leq (\alpha - 1)M \log^2 t. \end{aligned}$$

Luego, por la desigualdad triangular,

$$\begin{aligned}
|\zeta(\sigma + it)| &\geq |\zeta(\alpha + it)| - |\zeta(\sigma + it) - \zeta(\alpha + it)| \\
&\geq |\zeta(\alpha + it)| - (\alpha - 1)M \log^2 t \geq \frac{B(\alpha - 1)^{3/4}}{(\log t)^{1/4}} - (\alpha - 1)M \log^2 t.
\end{aligned}$$

Este resultado se verifica, si $1 \leq \sigma \leq \alpha$, y por (23) también se verifica para $\alpha \leq \sigma \leq 2$ puesto que $(\sigma - 1)^{3/4} \geq (\alpha - 1)^{3/4}$. Con otras palabras, si $1 \leq \sigma \leq 2$ y $t \geq e$ tenemos la desigualdad

$$|\zeta(\sigma + it)| \geq \frac{B(\alpha - 1)^{3/4}}{(\log t)^{1/4}} - (\alpha - 1)M \log^2 t$$

para todo α que satisfaga $1 < \alpha < 2$. Ahora α lo hacemos depender de t y elegimos α de forma que el primer término de la derecha sea igual a dos veces el segundo. Esto requiere que

$$\alpha = 1 + \left(\frac{B}{2M}\right)^4 \frac{1}{(\log t)^9}.$$

Es obvio que $\alpha > 1$ y también que $\alpha < 2$ si $t \geq t_0$ para cierto t_0 . Así pues, si $t \geq t_0$ y $1 \leq \sigma < 2$ tenemos

$$|\zeta(\sigma + it)| \geq (\alpha - 1)M \log^2 t = \frac{C}{(\log t)^7}.$$

Esta desigualdad se verifica asimismo con (quizás) una C diferente si $e \leq t \leq t_0$. Todo ello demuestra que $|\zeta(s)| \geq C \log^{-7} t$ para todo $\sigma \geq 1$, $t \geq e$, y, lo que nos proporciona es una cota superior de $|1/\zeta(s)|$. A fin de obtener la desigualdad relativa a $|\zeta'(s)/\zeta(s)|$ aplicamos el teorema 13.4 y obtenemos un factor extra $\log^2 t$. $\square$

13.7 TERMINACIÓN DE LA DEMOSTRACIÓN DEL TEOREMA DEL NÚMERO PRIMO

Estamos a punto de terminar la demostración del teorema del número primo. Necesitamos un resultado más de la teoría de funciones complejas que establezcamos en forma de lema.

Lema 4 Si $f(s)$ tiene un polo de orden k en $s = \alpha$, entonces el cociente $f'(s)/f(s)$ tiene un polo de primer orden en $s = \alpha$ con residuo $-k$.

DEMOSTRACIÓN. Tenemos $f(s) = g(s)/(s - \alpha)^k$, en donde g es analítica en α y $g(\alpha) \neq 0$. Luego, para todo s de un cierto entorno de α , tenemos

$$f'(s) = \frac{g'(s)}{(s - \alpha)^k} - \frac{kg(s)}{(s - \alpha)^{k+1}} = \frac{g(s)}{(s - \alpha)^k} \left\{ \frac{-k}{s - \alpha} + \frac{g'(s)}{g(s)} \right\}.$$

Por lo tanto

$$\frac{f'(s)}{f(s)} = \frac{-k}{s - \alpha} + \frac{g'(s)}{g(s)}.$$

Esto demuestra el lema ya que $g'(s)/g(s)$ es analítica en α . □

Teorema 13.8 La función

$$F(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$$

es analítica en $s = 1$.

DEMOSTRACIÓN. Por el lema 4, $-\zeta'(s)/\zeta(s)$ tiene un polo de primer orden en 1 con residuo 1, así como $1/(s-1)$. Luego su diferencia es analítica en $s = 1$. □

Teorema 13.9 Para $x \geq 1$ tenemos

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(1+it) e^{it \log x} dt,$$

en donde la integral $\int_{-\infty}^{\infty} |h(1+it)| dt$ converge. Por consiguiente, por el lema de Riemann-Lebesgue, tenemos

$$(24) \quad \psi_1(x) \sim x^2/2$$

y por lo tanto

$$\psi(x) \sim x \text{ cuando } x \rightarrow \infty.$$

DEMOSTRACIÓN. En el teorema 13.3 hemos demostrado que, si $c > 1$ y $x \geq 1$, tenemos

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2} \left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} x^{s-1} h(s) ds,$$

en donde

$$h(s) = \frac{1}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} \right).$$

La primera tarea que se nos plantea consiste en demostrar que podemos trasladar el camino de integración a la recta $\sigma = 1$. Para ello aplicamos el teorema de Cauchy al rectángulo dibujado en la figura 13.3. La integral de $x^{s-1} h(s)$ a lo largo de R

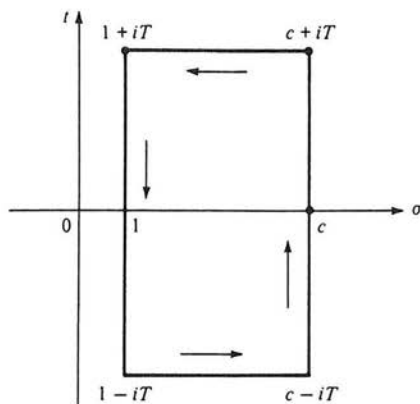


Figura 13.3

es 0 puesto que el integrando es analítico en el interior y sobre R . Ahora demostraremos que las integrales a lo largo de los segmentos horizontales tienden a 0 cuando $T \rightarrow \infty$. Dado que el integrando tiene el mismo valor absoluto en puntos conjugados, bastará considerar únicamente el segmento superior, $t = T$. En este segmento tenemos las acotaciones

$$\left| \frac{1}{s(s+1)} \right| \leq \frac{1}{T^2} \quad \text{y} \quad \left| \frac{1}{s(s+1)(s-1)} \right| \leq \frac{1}{T^3} \leq \frac{1}{T^2}.$$

Además existe una constante M tal que $|\zeta'(s)/\zeta(s)| \leq M \log^9 t$ si $\sigma \geq 1$ y $t \geq e$. Luego, si $T \geq e$, tenemos

$$|h(s)| \leq \frac{M \log^9 T}{T^2}$$

o sea que

$$\left| \int_1^c x^{s-1} h(s) ds \right| \leq \int_1^c x^{c-1} \frac{M \log^9 T}{T^2} d\sigma = M x^{c-1} \frac{\log^9 T}{T^2} (c-1).$$

Por consiguiente las integrales a lo largo de los segmentos horizontales tienden a 0 cuando $T \rightarrow \infty$, y por ello tenemos

$$\int_{c-\infty i}^{c+\infty i} x^{s-1} h(s) ds = \int_{1-\infty i}^{1+\infty i} x^{s-1} h(s) ds.$$

Sobre la recta $\sigma = 1$ escribimos $s = 1 + it$ y obtenemos

$$\frac{1}{2\pi i} \int_{1-\infty i}^{1+\infty i} x^{s-1} h(s) ds = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(1+it) e^{it \log x} dt.$$

Ahora observamos que

$$\int_{-\infty}^{\infty} |h(1+it)| dt = \int_{-e}^e + \int_e^{\infty} + \int_{-\infty}^{-e}.$$

En la integral de e a ∞ tenemos

$$|h(1+it)| \leq \frac{M \log^9 t}{t^2}$$

luego $\int_e^\infty |h(1+it)| dt$ converge. Análogamente, $\int_{-\infty}^{-e}$ converge, luego $\int_{-\infty}^\infty |h(1+it)| dt$ converge. Entonces podemos aplicar el lema de Riemann-Lebesgue para obtener $\psi_1(x) \sim x^2/2$. Por el teorema 13.1 esto implica $\psi(x) \sim x$ cuando $x \rightarrow \infty$, lo que termina la demostración del teorema del número primo. $\square$

13.8 REGIONES CARENTES DE CEROS DE $\zeta(s)$

La desigualdad $|1/\zeta(s)| < M \log^7 t$ que se ha demostrado en el teorema 13.7 para $\sigma \geq 1$ y $t \geq e$ se puede extender a la izquierda de la recta $\sigma = 1$. La acotación no se obtiene en una región vertical sino en una región semejante a la de la figura 13.2, en la que el borde izquierdo de la curva se aproxima a la recta $\sigma = 1$ asintóticamente cuando $t \rightarrow \infty$. La desigualdad implica la no anulación de $\zeta(s)$ en esta región. Con mayor precisión, tenemos:

Teorema 13.10 *Suponemos $\sigma \geq 1/2$. Entonces existen constantes $A > 0$ y $C > 0$ tales que*

$$|\zeta(\sigma + it)| > \frac{C}{\log^7 t}$$

siempre que

$$(25) \quad 1 - \frac{A}{\log^9 t} < \sigma \leq 1 \quad \text{y } t \geq e.$$

Esto implica que $\zeta(\sigma + it) \neq 0$ si σ y t satisfacen (25).

DEMOSTRACIÓN. La desigualdad triangular, junto con el teorema 13.7, nos dan, para un cierto $B > 0$

$$(26) \quad \begin{aligned} |\zeta(\sigma + it)| &\geq |\zeta(1 + it)| - |\zeta(1 + it) - \zeta(\sigma + it)| \\ &> \frac{B}{\log^7 t} - |\zeta(1 + it) - \zeta(\sigma + it)|. \end{aligned}$$

Para acotar el último término escribimos

$$|\zeta(1 + it) - \zeta(\sigma + it)| = \left| \int_\sigma^1 \zeta'(u + it) du \right| \leq \int_\sigma^1 |\zeta'(u + it)| du.$$

Como $t \geq e$, tenemos $\log^9 t \geq \log t$, luego $1 - (A/\log^9 t) \geq 1 - A/(\log t)$. Así pues, si σ satisface (25) para todo $A < 0$, podemos aplicar el teorema 13.4 para acotar $|\zeta'(u + it)|$, obteniendo

$$|\zeta(1 + it) - \zeta(\sigma + it)| \leq M(1 - \sigma)\log^2 t < M \log^2 t \frac{A}{\log^9 t} = \frac{MA}{\log^7 t}.$$

Utilizando este resultado en (26) obtenemos

$$|\zeta(\sigma + it)| > \frac{B - MA}{\log^7 t}.$$

Esta desigualdad se verifica para un cierto $B > 0$, todo $A > 0$ y un cierto $M > 0$ que depende de A . Un valor de M que sirva para un A sirve también para todo A más pequeño. Por consiguiente podemos elegir A ínfimo entre los que verifican $B - MA \geq 0$. Si en la última desigualdad hacemos $C = B - MA$ obtenemos $|\zeta(\sigma + it)| > C \log^{-7} t$ que prueba el teorema para todo σ y todo t que satisfagan

$$1 - \frac{A}{\log^9 t} < \sigma < 1, \quad \text{y } t \geq e.$$

Pero el resultado es válido también para $\sigma = 1$ por el teorema 13.7 con lo que se termina la demostración. $\square$

Sabemos que $\zeta(s) \neq 0$ si $\sigma \geq 1$, y la ecuación funcional

$$\zeta(s) = 2(2\pi)^{1-s} \Gamma(1-s) \operatorname{sen}\left(\frac{\pi s}{2}\right) \zeta(1-s)$$

prueba que $\zeta(s) \neq 0$ si $\sigma \leq 0$ excepto en los ceros $s = -2, -4, -6, \dots$ que se obtienen de la anulación de $\operatorname{sen}(\pi s/2)$. Son los llamados ceros «triviales» de $\zeta(s)$. El teorema que sigue prueba que, fuera de los ceros triviales, $\zeta(s)$ no posee sobre el eje real ningún otro cero.

Teorema 13.11 Si $\sigma > 0$ tenemos

$$(27) \quad (1 - 2^{1-s})\zeta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}.$$

Esto implica que $\zeta(s) < 0$ si s es real y $0 < s < 1$.

DEMOSTRACIÓN. Primero suponemos que $\sigma > 1$. Entonces tenemos

$$\begin{aligned}(1 - 2^{1-s})\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} - 2 \sum_{n=1}^{\infty} \frac{1}{(2n)^s} \\ &= (1 + 2^{-s} + 3^{-s} + \dots) - 2(2^{-s} + 4^{-s} + 6^{-s} + \dots) \\ &= 1 - 2^{-s} + 3^{-s} - 4^{-s} + 5^{-s} - 6^{-s} + \dots,\end{aligned}$$

que prueba (27) para $\sigma > 1$. Sin embargo, si $\sigma > 0$, la serie de la derecha converge, luego (27) también se verifica para $\sigma > 0$ por prolongación analítica.

Cuando s es real, la serie de (27) es una serie alternada que tiene suma positiva. Si $0 < s < 1$, el factor $(1 - 2^{1-s})$ es negativo, luego $\zeta(s)$ también es negativo. $\square$

13.9 LA HIPÓTESIS DE RIEMANN

En su famosa memoria de 8 páginas acerca de $\pi(x)$, publicada en 1859, Riemann [58] afirma que parece plausible que los ceros no triviales de $\zeta(s)$ pertenecen todos a la recta $\sigma = 1/2$, si bien no ha podido demostrarlo. La afirmación de que todos los ceros no triviales tienen parte real $1/2$ se conoce actualmente como *hipótesis de Riemann*. En 1900 Hilbert colocó el problema de demostrar o contradecir la hipótesis de Riemann en la lista de los problemas más importantes con que deberían enfrentarse los matemáticos del siglo veinte. Todavía hoy no ha sido resuelto.

La hipótesis de Riemann atrajo la atención de muchos de los matemáticos eminentes y se ha descubierto gran cantidad de resultados acerca de la distribución de los ceros de $\zeta(s)$. La ecuación funcional prueba que todos los ceros no triviales (si existe alguno) deben hallarse en la banda $0 < \sigma < 1$, llamada «banda crítica». Es fácil demostrar que los ceros se hallan distribuidos simétricamente respecto del eje real y de la «recta crítica» $\sigma = 1/2$.

En 1915, Hardy probó que hay una infinidad de ceros situados en la recta crítica. En 1921 Hardy y Littlewood demostraron que el número de ceros que hay en el segmento rectilíneo que une $1/2$ con $1/2 + (iT)$ es por lo menos AT para una cierta constante positiva A , si T es suficientemente grande. En 1942 Selberg lo perfeccionó probando que el número es por lo menos $AT \log T$ para un cierto $A > 0$. También se sabe que el número en la banda crítica con $0 < t < T$ es asintótico a $T \log T / 2\pi$ cuando $T \rightarrow \infty$, o sea que el resultado de Selberg prueba que una fracción positiva de los ceros está en la recta crítica. Recientemente (1974) Levinson ha demostrado que esta fracción es por lo menos $7/10$. Es decir que la constante del teorema de Selberg satisface $A \geq 7/20\pi$.

Extensos cálculos de Gram, Backlund, Lehmer, Haselgrove, Rosser, Yohe, Schoehfeld, y otros han demostrado que los tres primeros millones y medio de ceros por encima del eje real se hallan en la recta crítica. A despecho de que todo ello constituye una evidencia a favor de la hipótesis de Riemann los cálculos han revelado también ciertos fenómenos que sugieren que es muy posible que existan contraejemplos de la hipótesis de Riemann. Para una narración fascinante de la historia de los cálculos a gran escala concernientes a $\zeta(s)$, el lector puede consultar [17].

13.10 APLICACIÓN A LA FUNCIÓN DIVISOR

El teorema del número primo, a veces, es útil para estimar el orden de magnitud de funciones aritméticas multiplicativas. En esta sección lo utilizaremos para demostrar desigualdades para $d(n)$, número de divisores de n .

En el capítulo 3 hemos demostrado que el orden medio de $d(n)$ es $\log n$. Cuando n es primo tenemos $d(n) = 2$, por lo que el tamaño de $d(n)$ es tanto mayor cuantos más divisores tenga n . Suponemos que n es el producto de todos los números primos $\leq x$,

$$(28) \quad n = 2 \cdot 3 \cdot 5 \cdots p_{\pi(x)}.$$

Puesto que $d(n)$ es multiplicativa tenemos

$$d(n) = d(2)d(3) \cdots d(p_{\pi(x)}) = 2^{\pi(x)}.$$

Para x grande, $\pi(x)$ es aproximadamente $x/\log x$ y (28) implica

$$\log n = \sum_{p \leq x} \log p = \vartheta(x) \sim x$$

luego $2^{\pi(x)}$ es aproximadamente $2^{\log n / \log \log n}$. Ahora bien

$$2^{a \log n} = e^{a \log n \log 2} = n^{a \log 2}$$

luego $2^{\log n / \log \log n} = n^{\log 2 / \log \log n}$. Con otras palabras, cuando n es de la forma (28) entonces $d(n)$ es aproximadamente $2^{\log n / \log \log n} = n^{\log 2 / \log \log n}$.

Siguiendo esta idea un poco más cuidadosamente obtenemos las siguientes desigualdades para $d(n)$.

Teorema 13.12 Sea $\varepsilon > 0$. Entonces tenemos:

(a) Existe un entero $N(\varepsilon)$ tal que $n \geq N(\varepsilon)$ implica

$$d(n) < 2^{(1+\varepsilon) \log n / \log \log n} = n^{(1+\varepsilon) \log 2 / \log \log n}.$$

(b) Para una infinidad de n tenemos

$$d(n) > 2^{(1-\varepsilon) \log n / \log \log n} = n^{(1-\varepsilon) \log 2 / \log \log n}.$$

Nota. Estas desigualdades equivalen a la relación

$$\limsup_{n \rightarrow \infty} \frac{\log d(n) \log \log n}{\log n} = \log 2.$$

DEMOSTRACIÓN. Escribimos $n = p_1^{a_1} \dots p_k^{a_k}$, así que $d(n) = \prod_{i=1}^k (a_i + 1)$. Dividimos el producto en dos partes, separando los divisores primos $< f(n)$ de los $\geq f(n)$, en donde $f(n)$ se especificará más adelante. Entonces $d(n) = P_1(n)P_2(n)$ en donde

$$P_1(n) = \prod_{p_i < f(n)} (a_i + 1) \quad \text{y} \quad P_2(n) = \prod_{p_i \geq f(n)} (a_i + 1).$$

En el producto $P_2(n)$ utilizamos la desigualdad $(a + 1) \leq 2^a$ y obtenemos $P_2(n) \leq 2^{S(n)}$ en donde

$$S(n) = \sum_{\substack{i=1 \\ p_i \geq f(n)}}^k a_i.$$

Ahora bien

$$n = \prod_{i=1}^k p_i^{a_i} \geq \prod_{p_i \geq f(n)} p_i^{a_i} \geq \prod_{p_i \geq f(n)} f(n)^{a_i} = f(n)^{S(n)},$$

por lo tanto

$$\log n \geq S(n) \log f(n), \text{ luego } S(n) \leq \frac{\log n}{\log f(n)}.$$

Esto nos da

$$(29) \quad P_2(n) \leq 2^{\log n / \log f(n)}.$$

Para estimar $P_1(n)$ escribimos

$$P_1(n) = \exp \left\{ \sum_{p_i < f(n)} \log(a_i + 1) \right\}$$

y probamos que $\log(a_i + 1) < 2 \log \log n$ si n es suficientemente grande. De hecho tenemos

$$n \geq p_i^{a_i} \geq 2^{a_i}$$

por lo tanto

$$\log n \geq a_i \log 2, \quad \text{luego } a_i \leq \log n / \log 2.$$

Por consiguiente

$$1 + a_i \leq 1 + \frac{\log n}{\log 2} < (\log n)^2 \quad \text{si } n \geq n_1$$

para un cierto n_1 . Entonces $n \geq n_1$ implica $\log(1 + a_i) < \log(\log n)^2 = 2 \log \log n$. Esto nos da

$$P_1(n) < \exp \left\{ 2 \log \log n \sum_{p_i < f(n)} 1 \right\} \leq \exp \{ 2 \log \log n \pi(f(n)) \}.$$

Utilizando la desigualdad $\pi(x) < 6x/\log x$ (ver teorema 4.6) obtenemos

$$(30) \quad P_1(n) < \exp \left\{ \frac{12f(n) \log \log n}{\log f(n)} \right\} = 2^{c f(n) \log \log n / \log f(n)},$$

en donde $c = 12/\log 2$. Combinando (29) y (30) obtenemos $d(n) = P_1(n)P_2(n) < 2^{g(n)}$ en donde

$$g(n) = \frac{\log n + cf(n)\log \log n}{\log f(n)} = \frac{\log n}{\log \log n} \frac{1 + c \frac{f(n) \log \log n}{\log n}}{\frac{\log f(n)}{\log \log n}}.$$

Ahora elegimos $f(n)$ de forma que $f(n) \log \log n / \log n \rightarrow 0$ y además hacemos que $\log f(n) / \log \log n \rightarrow 1$ cuando $n \rightarrow \infty$. Para ello es suficiente tomar

$$f(n) = \frac{\log n}{(\log \log n)^2}.$$

Entonces

$$g(n) = \frac{\log n}{\log \log n} \frac{1 + o(1)}{1 + o(1)} = \frac{\log n}{\log \log n} (1 + o(1)) < (1 + \varepsilon) \frac{\log n}{\log \log n}$$

si $n \geq N(\varepsilon)$ para un cierto $N(\varepsilon)$. Esto prueba la parte (a).

Para demostrar la parte (b) tomamos un conjunto de enteros n que posean gran número de factores primos. Efectivamente, tomamos n igual al producto de todos los factores primos $\leq x$. Entonces $n \rightarrow \infty$ si, y sólo si, $x \rightarrow \infty$. Para ese n tenemos, por el teorema del número primo,

$$d(n) = 2^{\pi(x)} = 2^{(1+o(1))x/\log x}.$$

También, para este n , tenemos

$$\log n = \sum_{p \leq x} \log p = \vartheta(x) = x(1 + o(1))$$

luego

$$x = \frac{\log n}{1 + o(1)} = (1 + o(1)) \log n$$

por lo tanto

$$\begin{aligned}\log x &= \log \log n + \log(1 + o(1)) = \log \log n \left(1 + \frac{\log(1 + o(1))}{\log \log n}\right) \\ &= (1 + o(1)) \log \log n.\end{aligned}$$

Por consiguiente $x/\log x = (1 + o(1)) \log n / \log \log n$ y

$$d(n) = 2^{(1+o(1)) \log n / \log \log n}$$

para tal n . Pero $1 + o(1) > 1 - \varepsilon$ si $n \geq N(\varepsilon)$ para un cierto $N(\varepsilon)$ y esto prueba (b). $\square$

Nota. Como corolario del teorema 13.12 obtenemos la relación

$$(31) \quad d(n) = o(n^\delta)$$

para cada $\delta > 0$. Este resultado se puede obtener también sin necesidad de utilizar el teorema del número primo. (Ver ejercicio 13.13.)

13.11 APLICACIÓN A LA INDICATRIZ DE EULER

El tipo de razonamiento utilizado en la sección precedente se puede utilizar también para obtener desigualdades para $\varphi(n)$. Cuando n es primo tenemos $\varphi(n) = n - 1$. Cuando n posee gran número de factores primos, $\varphi(n)$ será mucho menor. Realmente si n es el producto de todos los primos $\leq x$ tenemos

$$\varphi(n) = n \prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

El teorema que sigue da el comportamiento asintótico de este producto cuando x es grande.

Teorema 13.13 *Existe una constante positiva c tal que, para $x \geq 2$,*

$$(32) \quad \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right).$$

Nota. Es posible demostrar que $c = e^{-C}$, en donde C es la constante de Euler (ver [31]).

DEMOSTRACIÓN. Si $P(x)$ designa el producto de (32), entonces $\log P(x) = \sum_{p \leq x} \log(1 - 1/p)$. Para estimar esta suma utilizamos el desarrollo en serie de potencias

$$-\log(1 - t) = t + \frac{t^2}{2} + \frac{t^3}{3} + \cdots + \frac{t^n}{n} + \cdots \quad (|t| < 1)$$

con $t = 1/p$. Si pasamos un término al otro miembro obtenemos, si $a_p = -\log(1 - 1/p) - 1/p$,

$$0 < a_p = \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots < \frac{1}{2} \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) = \frac{1}{2p(p-1)}.$$

Esta desigualdad prueba que la serie infinita

$$(33) \quad \sum_p a_p = \sum_p \left\{ -\log\left(1 - \frac{1}{p}\right) - \frac{1}{p} \right\}$$

converge, ya que está dominada por $\sum_{n=2}^{\infty} 1/n(n-1)$. Si B designa la suma de la serie dada en (33) tenemos

$$0 < B - \sum_{p \leq x} a_p = \sum_{p > x} a_p \leq \sum_{n \geq x} \frac{1}{n(n-1)} = - \sum_{n \geq x} \left(\frac{1}{n} - \frac{1}{n-1} \right) = O\left(\frac{1}{x}\right).$$

Luego

$$\sum_{p \leq x} a_p = B + O\left(\frac{1}{x}\right),$$

por lo tanto

$$-\log P(x) = \sum_{p \leq x} \frac{1}{p} + B + O\left(\frac{1}{x}\right).$$

Pero, por el teorema 4.12, la suma de la derecha es $\log \log x + A + O(1/\log x)$

así que

$$\log P(x) = -\log \log x - B - A + O\left(\frac{1}{\log x}\right).$$

Por consiguiente

$$P(x) = \exp\{\log P(x)\} = e^{-B-A} e^{-\log \log x} e^{O(1/\log x)}.$$

Sea ahora $c = e^{-B-A}$ y utilizando la desigualdad $e^u = 1 + u + O(u^2)$ para $0 < u < 1$ obtenemos

$$P(x) = \frac{c}{\log x} \left\{ 1 + O\left(\frac{1}{\log x}\right) \right\} = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right).$$

Esto termina la demostración. □

Teorema 13.14 Sea c la constante del teorema 13.13, y sea $\varepsilon > 0$.

(a) Existe un $N(\varepsilon)$ tal que

$$\varphi(n) \geq (1 - \varepsilon) \frac{cn}{\log \log n} \quad \text{para todo } n \geq N(\varepsilon).$$

(b) Para una infinidad de n tenemos

$$\varphi(n) \leq (1 + \varepsilon) \frac{cn}{\log \log n}.$$

Con otras palabras,

$$\liminf_{n \rightarrow \infty} \frac{\varphi(n) \log \log n}{n} = c.$$

DEMOSTRACIÓN. Primeramente probaremos (b). Tomamos $n = \prod_{p \leq x} p$. Entonces

$$\frac{\varphi(n)}{n} = \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{c}{\log x} + O\left(\frac{1}{\log^2 x}\right).$$

Pero $\log n = \theta(x) = (1 + o(1))x$, luego $\log \log n = (1 + o(1)) \log x$, por lo tanto

$$\frac{\varphi(n)}{n} = \frac{c(1 + o(1))}{\log \log n} + O\left(\frac{1}{(\log \log n)^2}\right) = \frac{c(1 + o(1))}{\log \log n} \leq (1 + \varepsilon) \frac{c}{\log \log n}$$

si $n \geq N(\varepsilon)$ para un $N(\varepsilon)$. Esto demuestra (b).

Para demostrar (a) tomamos $n > 1$ y escribimos

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right) = P_1(n)P_2(n)$$

en donde

$$P_1(n) = \prod_{\substack{p|n \\ p \leq \log n}} \left(1 - \frac{1}{p}\right), \quad y \quad P_2(n) = \prod_{\substack{p|n \\ p > \log n}} \left(1 - \frac{1}{p}\right).$$

Entonces

$$(34) \quad P_2(n) > \prod_{\substack{p|n \\ p > \log n}} \left(1 - \frac{1}{\log n}\right) = \left(1 - \frac{1}{\log n}\right)^{f(n)}$$

en donde $f(n)$ es el número de primos que dividen a n y exceden a $\log n$. Como

$$n \geq \prod_{p|n} p > \prod_{\substack{p|n \\ p > \log n}} p \geq (\log n)^{f(n)}$$

obtenemos $\log n > f(n) \log \log n$, por lo tanto $f(n) < \log n / \log \log n$. Pero al ser $1 - (1/\log n) < 1$, la desigualdad (34) nos da

$$(35) \quad P_2(n) > \left(1 - \frac{1}{\log n}\right)^{\log n / \log \log n} = \left\{ \left(1 - \frac{1}{\log n}\right)^{\log n} \right\}^{1 / \log \log n}$$

Ahora bien $(1 - (1/u))^u \rightarrow e^{-1}$ cuando $u \rightarrow \infty$ luego el último miembro de (35) tiende a 1 cuando $n \rightarrow \infty$. Por lo tanto (35) nos da

$$P_2(n) > 1 + o(1) \text{ cuando } n \rightarrow \infty.$$

Por consiguiente

$$\begin{aligned} \frac{\varphi(n)}{n} &= P_1(n)P_2(n) > (1 + o(1)) \prod_{\substack{p|n \\ p \leq \log n}} \left(1 - \frac{1}{p}\right) \geq (1 + o(1)) \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right) \\ &= (1 + o(1)) \frac{c}{\log \log n} (1 + o(1)) \geq (1 - \varepsilon) \frac{c}{\log \log n} \end{aligned}$$

si $n \geq N(\varepsilon)$. Esto demuestra la parte (a). □

13.12 EXTENSIÓN DE LA DESIGUALDAD DE PÓLYA PARA SUMAS DE CARACTERES

Terminamos este capítulo extendiendo la desigualdad de Pólya (teorema 8.21) a caracteres no principales arbitrarios. La demostración utiliza la estimación de la función divisor

$$d(n) = O(n^\delta)$$

obtenida en (31).

Teorema 13.15 Si χ es un carácter no principal mod k , entonces, para todo $x \geq 2$, tenemos

$$\sum_{m \leq x} \chi(m) = O(\sqrt{k} \log k).$$

DEMOSTRACIÓN. Si χ es primitivo, el teorema 8.21 demuestra que

$$\sum_{m \leq x} \chi(m) < \sqrt{k} \log k.$$

Sea ahora χ un carácter no principal arbitrario mod k y sea c el conductor de χ . Entonces $c|k$, $c < k$, y podemos escribir

$$\chi(m) = \psi(m)\chi_1(m)$$

en donde χ_1 es el carácter principal mod k y χ es un carácter primitivo mod c . Entonces

$$\begin{aligned}\sum_{m \leq x} \chi(m) &= \sum_{\substack{m \leq x \\ (m, k) = 1}} \psi(m) = \sum_{m \leq x} \psi(m) \sum_{d|(m, k)} \mu(d) = \sum_{m \leq x} \sum_{\substack{d|k \\ d|m}} \mu(d) \psi(m) \\ &= \sum_{d|k} \mu(d) \sum_{q \leq x/d} \psi(qd) = \sum_{d|k} \mu(d) \psi(d) \sum_{q \leq x/d} \psi(q).\end{aligned}$$

Luego

$$(36) \quad \left| \sum_{m \leq x} \chi(m) \right| \leq \sum_{d|k} |\mu(d) \psi(d)| \left| \sum_{q \leq x/d} \psi(q) \right| < \sqrt{c} \log c \sum_{d|k} |\mu(d) \psi(d)|$$

ya que ψ es primitivo mod c . En esta última suma cada factor $|\mu(d) \psi(d)|$ vale 0 ó 1. Si $|\mu(d) \psi(d)| = 1$ entonces $|\mu(d)| = 1$, luego d es un divisor de k sin factores cuadrados, es decir

$$d = p_1 p_2 \cdots p_r.$$

Además, $|\psi(d)| = 1$, luego $(d, c) = 1$, lo que significa que ningún factor primo p_i divide a c . Luego cada p_i divide a k/c , por lo tanto d divide a k/c . Con otras palabras

$$\sum_{d|k} |\mu(d) \psi(d)| \leq \sum_{d|k/c} 1 = d\left(\frac{k}{c}\right) = O\left(\left(\frac{k}{c}\right)^\delta\right)$$

para cada $\delta > 0$. En particular, $d(k/c) = O(\sqrt{k/c})$, luego (36) implica

$$\sum_{m \leq x} \chi(m) = O\left(\sqrt{\frac{k}{c}} \sqrt{c} \log c\right) = O(\sqrt{k} \log c) = O(\sqrt{k} \log k). \quad \square$$

Ejercicios del capítulo 13

1. Chebyshev probó que, si $\psi(x)/x$ tiende a un límite cuando $x \rightarrow \infty$ entonces este límite es igual a 1. Una demostración fue indicada ya en el ejercicio 4.26. Este ejercicio proporciona otra demostración basada en la identidad

$$(37) \quad -\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(x)}{x^{s+1}} dx, \quad (\sigma > 1)$$

dada en el ejercicio 11.1(d).

(a) Probar que $(1-s)\zeta'(s)/\zeta(s) \rightarrow 1$ cuando $s \rightarrow 1$.

(b) Sea $\delta = \liminf_{x \rightarrow \infty} (\psi(x)/x)$. Dado $\varepsilon > 0$, elegimos $N = N(\varepsilon)$ tal que $x \geq N$ implique $\psi(x) \leq (\delta + \varepsilon)x$. Tomamos s real, $1 < s \leq 2$, descomponemos la integral de (37) en dos partes, $\int_1^N + \int_N^\infty$, y acotamos cada parte a fin de obtener la desigualdad

$$-\frac{\zeta'(s)}{\zeta(s)} \leq C(\varepsilon) + \frac{s(\delta + \varepsilon)}{s-1},$$

en donde $C(\varepsilon)$ es una constante independiente de s . Utilizar (a) para deducir que $\delta \geq 1$.

(c) Sea $\gamma = \liminf_{x \rightarrow \infty} (\psi(x)/x)$ y utilizar un razonamiento análogo para deducir que $\gamma \leq 1$.

Por consiguiente, si $\psi(x)/x$ tiende a un límite cuando $x \rightarrow \infty$, entonces $\gamma = \delta = 1$.

2. Sea $A(x) = \sum_{n \leq x} a(n)$, en donde

$$a(n) = \begin{cases} 0 & \text{si } n \neq \text{una potencia de primo,} \\ \frac{1}{k} & \text{si } n = p^k. \end{cases}$$

Probar que $A(x) = \pi(x) + O(\sqrt{x} \log \log x)$.

3. (a) Si $c > 1$ y $x \neq$ entero, probar que, si $x > 1$,

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \log \zeta(s) \frac{x^s}{s} ds = \pi(x) + \frac{1}{2} \pi(x^{1/2}) + \frac{1}{3} \pi(x^{1/3}) + \dots$$

(b) Probar que el teorema del número primo es equivalente a la relación asintótica

$$\frac{1}{2\pi i} \int_{c-\infty i}^{c+\infty i} \log \zeta(s) \frac{x^s}{s} ds \sim \frac{x}{\log x} \quad \text{cuando } x \rightarrow \infty.$$

Una demostración del teorema del número primo basada en esta relación fue establecida por Landau en 1903.

4. Sea $M(x) = \sum_{n \leq x} \mu(n)$. Se desconoce el orden exacto de magnitud de $M(x)$ para x grande. En el capítulo 4 probábamos que el teorema del número primo es equivalente a la relación $M(x) = o(x)$ cuando $x \rightarrow \infty$. Este ejercicio relaciona el orden de magnitud de $M(x)$ con la hipótesis de Riemann.

Suponemos que existe una constante positiva θ tal que

$$M(x) = O(x^\theta) \quad \text{para } x \geq 1.$$

Probar que la fórmula

$$\frac{1}{\zeta(s)} = s \int_1^\infty \frac{M(x)}{x^{s+1}} dx,$$

que es válida para $\sigma > 1$ (ver ejercicio 11,1(c)) también es válida para $\sigma > \theta$. Deducir que $\zeta(s) \neq 0$ para $\sigma > \theta$. En particular, esto prueba que la relación $M(x) = O(x^{1/2+\varepsilon})$ para cada $\varepsilon > 0$ implica la hipótesis de Riemann. También se puede demostrar que la hipótesis de Riemann implica $M(x) = O(x^{1/2+\varepsilon})$ para cada $\varepsilon > 0$. (Ver Titchmarsh [69], p. 315.)

5. Probar el siguiente lema, que es análogo al lema 2. Sea

$$A_1(x) = \int_1^x \frac{A(u)}{u} du,$$

en donde $A(u)$ es una función creciente no negativa para $u \geq 1$. Si, para un $c > 0$ y un $L > 0$, tenemos la fórmula asintótica

$$A_1(x) \sim Lx^c \text{ cuando } x \rightarrow \infty,$$

entonces es

$$A(x) \sim cLx^c \text{ cuando } x \rightarrow \infty.$$

6. Probar que

$$\frac{1}{2\pi i} \int_{2-\infty i}^{2+\infty i} \frac{y^s}{s^2} ds = 0 \quad \text{si } 0 < y < 1.$$

¿Cuál es el valor de esta integral si $y \geq 1$?

7. Expresar

$$\frac{1}{2\pi i} \int_{2-\infty i}^{2+\infty i} \frac{x^s}{s^2} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) ds$$

como una suma finita que contenga a $\Lambda(n)$

8. Sea χ un carácter cualquiera de Dirichlet mod k y χ_1 el carácter principal. Definimos

$$F(\sigma, t) = 3 \frac{L'}{L}(\sigma, \chi_1) + 4 \frac{L'}{L}(\sigma + it, \chi) + \frac{L'}{L}(\sigma + 2it, \chi^2).$$

Si $\sigma > 1$, probar que $F(\sigma, t)$ tiene parte real igual a

$$- \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma} \operatorname{Re}\{3\chi_1(n) + 4\chi(n)n^{-it} + \chi^2(n)n^{-2it}\}$$

y deducir que $\operatorname{Re} F(\sigma, t) \leq 0$.

9. Suponemos que $L(s, \chi)$ tiene un cero de orden $m \geq 1$ en $s = 1 + it$. Probar que, para este t , tenemos:

$$(a) \frac{L'}{L}(\sigma + it, \chi) = \frac{m}{\sigma - 1} + O(1) \quad \text{cuando } \sigma \rightarrow 1 +,$$

y

- (b) existe un entero $r \geq 0$ tal que

$$\frac{L'}{L}(\sigma + 2it, \chi^2) = \frac{r}{\sigma - 1} + O(1) \quad \text{cuando } \sigma \rightarrow 1 +,$$

excepto cuando $\chi^2 = \chi_1$ y $t = 0$.

10. Utilizar los ejercicios 8 y 9 para demostrar que

$$L(1 + it, \chi) \neq 0 \quad \text{para todo real } t \text{ si } \chi^2 \neq \chi_1$$

y que

$$L(1 + it, \chi) \neq 0 \quad \text{para todo real } t \neq 0 \text{ si } \chi^2 = \chi_1.$$

[Indicación: Considerar $F(\sigma, t)$ cuando $\sigma \rightarrow 1 +$.]

11. Para toda función aritmética $f(n)$, probar que las siguientes afirmaciones son equivalentes:

(a) $f(n) = O(n^\varepsilon)$ para cada $\varepsilon > 0$ y todo $n \geq n_1$.

(b) $f(n) = o(n^\delta)$ para cada $\delta > 0$ cuando $n \rightarrow \infty$.

12. Sea f una función multiplicativa tal que, si p es primo, entonces

$$f(p^m) \rightarrow 0 \quad \text{cuando } p^m \rightarrow \infty$$

Es decir, para cada $\varepsilon > 0$, existe un $N(\varepsilon)$ tal que $|f(p^m)| < \varepsilon$ si $p^m > N(\varepsilon)$. Probar que $f(n) \rightarrow 0$ cuando $n \rightarrow \infty$.

[Indicación: Existe una constante $A > 0$ tal que $|f(p^m)| < A$ para todo primo p y todo $m \geq 0$, y una constante $B > 0$ tal que $|f(p^m)| < 1$ si $p^m > B$.]

13. Si $\alpha \geq 0$, sea $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Probar que, para cada $\delta > 0$, tenemos

$$\sigma_\alpha(n) = o(n^{\alpha+\delta}) \quad \text{cuando } n \rightarrow \infty.$$

[Indicación: Utilizar el ejercicio 12.]

Capítulo 14

Particiones

14.1 INTRODUCCIÓN

Hasta ahora este libro ha tratado principalmente de la *teoría multiplicativa de números*, un estudio de las funciones aritméticas relacionadas con la descomposición de enteros en factores primos. Ahora se vuelve hacia otra rama de la Teoría de números llamada *teoría aditiva de números*. Un problema básico en este contexto consiste en expresar un entero positivo dado n como suma de los enteros de un cierto conjunto A , dado de antemano,

$$A = \{a_1, a_2, \dots\},$$

en donde los elementos a_i son números especiales tales como primos, cuadrados, cubos, números triangulares, etc. Cada representación de n como suma de elementos de A se llama *partición* de n y nos interesa la función $A(n)$ que cuenta el número de particiones de n en sumandos de A . Ilustraremos el problema con algunos ejemplos famosos.

Conjetura de Goldbach. *Todo número par $n > 4$ es suma de dos primos impares.*

En este ejemplo $A(n)$ es el número de soluciones de la ecuación

$$(1) \quad n = p_1 + p_2,$$

en donde los p_i son primos impares. La afirmación de Goldbach es que $A(n) \geq 1$ para todo par $n > 4$. Esta conjetura data de 1742 y, en esta fecha, quedó sin decidir. En 1937 el matemático ruso Vinogradov probó que cada entero par suficientemente grande es la suma de tres primos impares. En 1966 el matemático chino Chen Jing-run demostró que cada número par suficientemente grande es la suma de un primo más un número que no posee más de dos divisores primos. (Ver [10].)

Representación por cuadrados. Para un entero dado $k \geq 2$ consideramos la función de partición $r_k(n)$ que cuenta el número de soluciones de la ecuación

$$(2) \quad n = x_1^2 + \cdots + x_k^2,$$

en donde los x_i pueden ser positivos, negativos o nulos, y el orden de los sumandos se toma de acuerdo con el orden creciente de su valor.

Para $k = 2, 4, 6$ ó 8 , Jacobi [34] expresó $r_k(n)$ en términos de las funciones divisor. Por ejemplo, demostró que

$$r_2(n) = 4\{d_1(n) - d_3(n)\},$$

en donde $d_1(n)$ y $d_3(n)$ son el número de divisores de n congruentes con 1 y 3 mod 4, respectivamente. Entonces, $r_2(5) = 8$ puesto que ambos divisores, 1 y 5, son congruentes con 1 mod 4. De hecho existen cuatro representaciones dadas por

$$5 = 2^2 + 1^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2 = 2^2 + (-1)^2,$$

y otras cuatro con el orden de los sumandos invertido.

Para $k = 4$ Jacobi probó que

$$\begin{aligned} r_4(n) &= \sum_{d|n} d = 8\sigma(n) \quad \text{si } n \text{ es impar,} \\ &= 24 \sum_{\substack{d|n \\ d \text{ impar}}} d \quad \text{si } n \text{ es par.} \end{aligned}$$

Las fórmulas para $r_6(n)$ y $r_8(n)$ son algo más complicadas pero del mismo tipo general. (Ver [14].)

Se han obtenido hasta el momento fórmulas exactas para $k = 3, 5$, ó 7 ; contienen la extensión de Jacobi del símbolo de Legendre para restos cuadráticos. Por ejemplo, si n es impar sabemos que

$$\begin{aligned} r_3(n) &= 24 \sum_{m \leq n/4} (m|n) \quad \text{si } n \equiv 1 \pmod{4} \\ &= 8 \sum_{m \leq n/2} (m|n) \quad \text{si } n \equiv 3 \pmod{4}, \end{aligned}$$

en donde ahora los números x_1, x_2, x_3 de (2) se han tomado primos entre sí.

Para valores grandes de k , el análisis de $r_k(n)$ es considerablemente más complicado. Existe mucha literatura sobre este tema con contribuciones de Mordell, Hardy, Littlewood, Ramanujan, y muchos otros. Para $k \geq 5$ sabemos que $r_k(n)$ se puede expresar mediante una fórmula asintótica de la forma

$$(3) \quad r_k(n) = \rho_k(n) + R_k(n),$$

en donde $\rho_k(n)$ es el término principal, dado por la serie infinita

$$\rho_k(n) = \frac{\pi^{k/2} n^{k/2-1}}{\Gamma\left(\frac{k}{2}\right)} \sum_{q=1}^{\infty} \sum_{\substack{h=1 \\ (h,q)=1}}^q \left(\frac{G(h;q)}{q}\right)^k e^{-2\pi i n h/q},$$

y $R_k(n)$ es un resto de orden menor. La serie de $\rho_k(n)$ se llama *serie singular* y los números $G(h;q)$ son las sumas cuadráticas de Gauss,

$$G(h;q) = \sum_{r=1}^q e^{2\pi i h r^2/q}.$$

En 1917, Mordell observó que $r_k(n)$ es el coeficiente de x^n en el desarrollo en serie de la k -ésima potencia de la serie

$$\vartheta = 1 + 2 \sum_{n=1}^{\infty} x^{n^2}.$$

La función ϑ se halla relacionada con las funciones modulares elípticas que juegan un papel realmente importante en la obtención de (3).

Problema de Waring. *Determinar si para un entero positivo dado k , existe un entero s (que dependa sólo de k) tal que la ecuación*

$$(4) \quad n = x_1^k + x_2^k + \cdots + x_s^k$$

tenga soluciones para cada $n \geq 1$.

El problema se conoce con el nombre del matemático inglés E. Waring que estableció en 1770 (sin demostración y con limitada evidencia numérica) que cada n es la suma de 4 cuadrados, de 9 cubos, de 19 cuartas potencias, etc. En este ejemplo la función de partición $A(n)$ es el número de soluciones de (4), y el problema consiste en decidir si existe un número s tal que $A(n) \geq 1$ para todo n .

Si s existe para un k dado entonces existe un mínimo valor de s y éste se designa $g(k)$. Lagrange probó la existencia de $g(2)$ en 1770 y, en los 139 años siguientes, se probó la existencia de $g(k)$ para $k = 3, 4, 5, 6, 7, 8$ y 10. En 1909, Hilbert demostró la existencia de $g(k)$ para todo k mediante un argumento inductivo pero no determinó su valor numérico para cualquier k . Actualmente se conoce el valor exacto de $g(k)$ para cada k excepto para $k = 4$. Hardy y Littlewood hallaron una fórmula asintótica para el número de soluciones de (4) en términos de una serie singular análoga a la de (3). Para una reseña histórica del problema de Waring, ver W. J. Ellison [18].

Particiones no restrictivas

Uno de los problemas fundamentales en la teoría aditiva de números es el de las particiones no restrictivas. El conjunto de los sumandos consta de todos los enteros positivos, y la función de partición que se estudia es el número de formas en que podemos descomponer n como suma de enteros positivos $\leq n$, esto es, el número de soluciones de

$$(5) \quad n = a_{i_1} + a_{i_2} + \cdots$$

El número de sumandos no se halla sometido a ninguna restricción, se permite repetir sumandos, y el orden de los sumandos no se toma en cuenta. La función de partición correspondiente se designa $p(n)$ y se llama *función de partición no restrictiva*, o simplemente *función de partición*. Los sumandos se llaman *partes*. Por ejemplo, existen exactamente cinco particiones de 4, dadas por

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1,$$

luego $p(4) = 5$. Análogamente, $p(5) = 7$, siendo las particiones de 5

$$\begin{aligned} 5 &= 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1. \end{aligned}$$

El resto de este capítulo lo dedicaremos al estudio de $p(n)$ y de funciones relacionadas.

14.2 REPRESENTACIÓN GEOMÉTRICA DE LAS PARTICIONES

Existe un método simple para representar particiones geoméricamente utilizando una disposición de puntos reticulares que llamaremos *grafo*. Por ejemplo, la partición de 15 dada por

$$6 + 3 + 3 + 2 + 1$$

se puede representar por medio de 15 puntos colocados en cinco filas tal como sigue:

$$\begin{array}{cccccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & & & & \\ \cdot & & & & & \end{array}$$

Si leemos este grafo verticalmente obtenemos otra partición de 15,

$$5 + 4 + 3 + 1 + 1 + 1.$$

Estas dos particiones son *conjugadas*. Nótese que la parte *más larga* de una de ellas es igual al *número de partes* de la otra. Entonces tenemos el teorema que sigue.

Teorema 14.1 *El número de particiones de n en m partes es igual al número de particiones de n en partes tales que la mayor sea m .*

Se pueden demostrar muchos teoremas combinando simplemente argumentos que involucren grafos, y más adelante daremos una ilustración muy bonita de este método. Sin embargo, los resultados profundos de la teoría de las particiones requiere un tratamiento analítico más profundo, al que ahora vamos a dedicarnos.

14.3 FUNCIONES GENERADORAS DE PARTICIONES

Una función $F(s)$ definida por una serie de Dirichlet $F(s) = \sum f(n)n^{-s}$ se llama *función generadora* de los coeficientes $f(n)$. Las series de Dirichlet son útiles para generar funciones en la teoría multiplicativa de números en virtud de la relación

$$n^{-s}m^{-s} = (nm)^{-s}.$$

En la teoría aditiva de números es más conveniente generar funciones utilizando su representación en serie de potencias,

$$F(x) = \sum f(n)x^n$$

ya que $x^n x^m = x^{n+m}$. El teorema que sigue pone de manifiesto una función generadora de la función de partición $p(n)$.

Teorema 14.2 Euler. Para $|x| < 1$ tenemos

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = \sum_{n=0}^{\infty} p(n)x^n,$$

en donde $p(0) = 1$.

DEMOSTRACIÓN. En primer lugar damos una deducción formal de esta identidad, ignorando las cuestiones de convergencia, y después damos una demostración más rigurosa.

Si cada factor del producto lo desarrollamos en serie de potencias (una serie geométrica) obtenemos

$$\prod_{n=1}^{\infty} \frac{1}{1-x^n} = (1+x+x^2+\cdots)(1+x^2+x^4+\cdots)(1+x^3+x^6+\cdots)\cdots$$

Ahora multiplicamos las series de la derecha, tratándolas como si fuesen polinomios y agrupándolas según las potencias de x a fin de obtener una serie de potencias de la forma

$$1 + \sum_{k=1}^{\infty} a(k)x^k.$$

Queremos demostrar que $a(k) = p(k)$. Suponemos que hemos tomado el término x^{k_1} de la primera serie, el término x^{2k_2} de la segunda, el término x^{3k_3} de la tercera, ..., y el término x^{mk_m} de la m -ésima, en donde cada $k_i \geq 0$. Su producto es

$$x^{k_1} x^{2k_2} x^{3k_3} \dots x^{mk_m} = x^k,$$

en donde

$$k = k_1 + 2k_2 + 3k_3 + \dots + mk_m.$$

Este resultado se puede escribir también como sigue:

$$k = (1 + 1 + \dots + 1) + (2 + 2 + \dots + 2) + \dots + (m + m + \dots + m),$$

en donde el primer paréntesis contiene k_1 unos, el segundo k_2 doses, y así sucesivamente. Esta es una partición de k en sumandos positivos. Entonces, cada partición de k producirá uno de los términos x^k y, recíprocamente, cada término x^k procede de una partición conveniente de k . Por consiguiente $a(k)$, el coeficiente de x^k , es igual a $p(k)$, el número de particiones de k .

El razonamiento anterior no constituye una demostración rigurosa ya que se han ignorado las cuestiones de convergencia y además hemos multiplicado conjuntamente una infinidad de series geométricas, tratándolas como si fuesen polinomios. Sin embargo no es difícil transformar las ideas anteriores en una demostración rigurosa.

A este fin imponemos que x pertenezca al intervalo $0 \leq x < 1$ e introducimos dos funciones,

$$F_m(x) = \prod_{k=1}^m \frac{1}{1-x^k}, \quad y \quad F(x) = \prod_{k=1}^{\infty} \frac{1}{1-x^k} = \lim_{m \rightarrow \infty} F_m(x).$$

El producto que define $F(x)$ converge absolutamente si $0 \leq x < 1$, puesto que su inversa $\prod (1-x^k)$ converge absolutamente (ya que la serie $\sum x^k$ converge absolutamente). Obsérvese además que, para cada x fijo, la sucesión $\{F_m(x)\}$ es creciente puesto que

$$F_{m+1}(x) = \frac{1}{1-x^{m+1}} F_m(x) \geq F_m(x).$$

Luego $F_m(x) \leq F(x)$ para cada x fijo, $0 \leq x < 1$, y cada m . Pero $F_m(x)$ es el producto de un número finito de series absolutamente convergentes. Por consiguiente también ella será una serie absolutamente convergente que podemos escribir en la forma

$$F_m(x) = 1 + \sum_{k=1}^{\infty} p_m(k)x^k.$$

Aquí $p_m(k)$ es el número de soluciones de la ecuación

$$k = k_1 + 2k_2 + \cdots + mk_m.$$

Con otras palabras, $p_m(k)$ es el número de particiones de k en partes que no exceden m . Si $m \geq k$, entonces $p_m(k) = p(k)$. Por consiguiente, en todos los casos, tenemos

$$p_m(k) \leq p(k)$$

con igualdad cuando $m \geq k$. Con otras palabras, tenemos

$$\lim_{m \rightarrow \infty} p_m(k) = p(k).$$

Ahora descomponemos las series relativas a $F_m(x)$ en dos partes,

$$\begin{aligned} F_m(x) &= \sum_{k=0}^m p_m(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k \\ &= \sum_{k=0}^m p(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k. \end{aligned}$$

Puesto que $x \geq 0$ tenemos

$$\sum_{k=0}^m p(k)x^k \leq F_m(x) \leq F(x).$$

Ello demuestra que la serie $\sum_{k=0}^{\infty} p(k)x^k$ converge. Sin embargo, puesto que $p_m(k) \leq p(k)$, tenemos

$$\sum_{k=0}^{\infty} p_m(k)x^k \leq \sum_{k=0}^{\infty} p(k)x^k \leq F(x)$$

luego, para cada x fijo, la serie $\sum p_m(k)x^k$ converge uniformemente en m . Si hacemos que $m \rightarrow \infty$ obtenemos

$$F(x) = \lim_{m \rightarrow \infty} F_m(x) = \lim_{m \rightarrow \infty} \sum_{k=0}^{\infty} p_m(k)x^k = \sum_{k=0}^{\infty} \lim_{m \rightarrow \infty} p_m(k)x^k = \sum_{k=0}^{\infty} p(k)x^k,$$

que demuestra la identidad de Euler para $0 \leq x < 1$. Por prolongación analítica la extendemos al disco unidad $|x| < 1$.

Tabla 14.1 Funciones generadoras

Función generadora	El número de particiones de n en partes que son
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m-1}}$	impares
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m}}$	pares
$\prod_{m=1}^{\infty} \frac{1}{1-x^{m^2}}$	cuadrados
$\prod_p \frac{1}{1-x^p}$	primos
$\prod_{m=1}^{\infty} (1+x^m)$	desiguales
$\prod_{m=1}^{\infty} (1+x^{2m-1})$	impares y desiguales
$\prod_{m=1}^{\infty} (1+x^{2m})$	pares y desiguales
$\prod_{m=1}^{\infty} (1+x^{m^2})$	cuadrados diferentes
$\prod_p (1+x^p)$	primos diferentes

Mediante razonamientos análogos podemos obtener funciones generadoras de muchas otras funciones de partición. En la tabla 14.1 mencionamos sólo algunos ejemplos.

14.4 EL TEOREMA DE EULER DE LOS NÚMEROS PENTAGONALES

A continuación consideramos la función de partición generada por el producto $\prod (1 - x^m)$, inversa de la función generadora de $p(n)$. Escribimos

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} a(n)x^n.$$

Para expresar $a(n)$ como una función de partición observamos que cada partición de n partes desiguales produce un término x^n en el segundo miembro con coeficiente $+1$ o -1 . El coeficiente es $+1$ si x^n es el producto de un número par de términos, y -1 en los demás casos. Por consiguiente,

$$a(n) = p_e(n) - p_o(n),$$

en donde $p_e(n)$ es el número de particiones de n en un número par de partes desiguales, y $p_o(n)$ es el número de particiones en un número impar de partes desiguales. Euler demostró que $p_e(n) = p_o(n)$ para todo n excepto para los que pertenecen a un conjunto especial llamado de los *números pentagonales*.

Los números pentagonales 1, 5, 12, 22, ... ya fueron mencionados en la introducción histórica. Están relacionados con los pentágonos dibujados en la figura 14.1.



Figura 14.1

Estos números son también las sumas parciales de los términos de la progresión aritmética

$$1, 4, 7, 10, 13, \dots, 3n + 1, \dots$$

Si $\omega(n)$ designa la suma de los n primeros términos de esta progresión entonces

$$\omega(n) = \sum_{k=0}^{n-1} (3k + 1) = \frac{3n(n-1)}{2} + n = \frac{3n^2 - n}{2}.$$

Los números $\omega(n)$ y $\omega(-n) = (3n^2 + n)/2$ se llaman *números pentagonales*.

Teorema 14.3 Teorema de los números pentagonales de Euler. Si $|x| < 1$ tenemos

$$\begin{aligned} \prod_{m=1}^{\infty} (1 - x^m) &= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \dots \\ &= 1 + \sum_{n=1}^{\infty} (-1)^n \{x^{\omega(n)} + x^{\omega(-n)}\} = \sum_{n=-\infty}^{\infty} (-1)^n x^{\omega(n)}. \end{aligned}$$

DEMOSTRACIÓN. Primero probaremos el resultado para $0 \leq x < 1$ y después lo extenderemos al disco $|x| < 1$ por prolongación analítica. Definimos $P_0 = S_0 = 1$ y, para $n \geq 1$, consideramos

$$P_n = \prod_{r=1}^n (1 - x^r) \quad \text{y} \quad S_n = 1 + \sum_{r=1}^n (-1)^r \{x^{\omega(r)} + x^{\omega(-r)}\}.$$

El producto infinito $\prod (1 - x^m)$ converge, luego $P_n \rightarrow \prod (1 - x^m)$ cuando $n \rightarrow \infty$. Probaremos (utilizando el método de Shanks [63]) que

$$(6) \quad |S_n - P_n| \leq nx^{n+1}.$$

Puesto que $nx^{n+1} \rightarrow 0$ cuando $n \rightarrow \infty$ esto prueba la identidad de Euler para $0 \leq x < 1$.

Para probar (6) consideramos $g(r) = r(r+1)/2$ e introducimos las sumas

$$F_n = \sum_{r=0}^n (-1)^r \frac{P_n}{P_r} x^{rn+g(r)}.$$

En primer lugar probaremos que F_n es una forma disfrazada de S_n . Es fácil comprobar que $F_1 = S_1 = 1 - x - x^2$. Por consiguiente, si vemos que

$$F_n - F_{n-1} = S_n - S_{n-1}, \quad \text{o que } F_n - S_n = F_{n-1} - S_{n-1},$$

habremos demostrado que, para todo $n \geq 1$, $F_n = S_n$. Ahora bien

$$F_n - F_{n-1} = \sum_{r=0}^n (-1)^r \frac{P_n}{P_r} x^{rn+g(r)} - \sum_{r=0}^{n-1} (-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}.$$

En la primera suma escribimos $P_n = (1 - x^n)P_{n-1}$ y separamos el término con $r = n$. Entonces distribuimos la diferencia $1 - x^n$ y obtenemos

$$\begin{aligned} F_n - F_{n-1} &= (-1)^n x^{n^2+g(n)} + \sum_{r=0}^{n-1} (-1)^r \frac{P_{n-1}}{P_r} x^{rn+g(r)} \\ &\quad - \sum_{r=0}^{n-1} (-1)^r \frac{P_{n-1}}{P_r} x^{(r+1)n+g(r)} - \sum_{r=0}^{n-1} (-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}. \end{aligned}$$

Ahora combinamos la primera y la tercera suma y observamos que el término con $r = 0$ se anula. En el segundo sumando desplazamos los índices y obtenemos

$$\begin{aligned} F_n - F_{n-1} &= (-1)^n x^{n^2+g(n)} + \sum_{r=1}^{n-1} (-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)} (x^r - 1) \\ &\quad - \sum_{r=1}^n (-1)^{r-1} \frac{P_{n-1}}{P_{r-1}} x^{rn+g(r-1)}. \end{aligned}$$

Pero $(x^r - 1)/P_r = -1/P_{r-1}$ y $r(n-1) + g(r) = rn + g(r-1)$ luego los dos últimos sumandos se anulan término a término excepto para el término con $r = n$ de la segunda suma. Así, obtenemos

$$F_n - F_{n-1} = (-1)^n x^{n^2+g(n)} + (-1)^n x^{n^2+g(n-1)}.$$

Pero

$$n^2 + g(n) = n^2 + \frac{n(n+1)}{2} = \omega(-n) \quad \text{y} \quad n^2 + g(n-1) = \omega(n),$$

luego

$$F_n - F_{n-1} = (-1)^n \{x^{\omega(n)} + x^{\omega(-n)}\} = S_n - S_{n-1},$$

y entonces $F_n = S_n$ para todo $n \geq 1$. En la suma que define F_n el primer término es P_n luego

$$(7) \quad F_n = P_n + \sum_{r=1}^n (-1)^r \frac{P_n}{P_r} x^{rn+g(r)}.$$

Obsérvese que $0 < P_n/P_r \leq 1$ ya que $0 \leq x < 1$. Además, cada factor $x^{rn+g(r)} \leq x^{n+1}$, luego la suma de la derecha de (7) está acotada superiormente por nx^{n+1} . Por consiguiente $|F_n - P_n| \leq nx^{n+1}$ y, dado que $F_n = S_n$, esto demuestra (6) y termina la demostración de la identidad de Euler. $\square$

14.5 DEMOSTRACIÓN COMBINATORIA DEL TEOREMA DE LOS NÚMEROS PENTAGONALES DE EULER

Euler demostró su teorema de los números pentagonales por inducción en 1750. Más tarde Legendre en 1830 y Jacobi en 1846 obtuvieron otras demostraciones. Esta sección describe una demostración combinatorial realmente notable dada por F. Franklin [22] en 1881.

Ya hemos observado que

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} \{p_e(n) - p_o(n)\} x^n,$$

en donde $p_e(n)$ es el número de particiones de n en un número *par* de partes desiguales, y $p_o(n)$ es el número de particiones de n en un número *impar* de partes desiguales. Franklin utilizó la representación gráfica de las particiones mediante puntos reticulares para demostrar que existe una correspondencia uno a uno entre las particiones de n en un número par de partes desiguales y las particiones de n

en un número impar de partes desiguales, de modo que $p_e(n) = p_a(n)$, excepto cuando n es un número pentagonal.

Consideremos el grafo de una partición de n partes desiguales. Decimos que el grafo se halla en *forma estándar* si las partes se colocan en orden decreciente, tal como ilustra el ejemplo de la figura 14.2. La longitud del segmento rectilíneo que contiene los puntos de la última fila se llama la *base* del grafo, y el número de puntos reticulares de la base se designará por b . Luego, $b \geq 1$. El segmento rectilíneo más largo de 45° de inclinación que une el último punto de la primera fila con otros puntos del grafo se denomina *rampa* del grafo, y el número de puntos reticulares que se hallan sobre la rampa se designa por s . Luego $s \geq 1$. En la figura 14.2 tenemos $b = 2$ y $s = 4$.

Ahora definimos dos operaciones A y B en este grafo. La operación A mueve los puntos de la base de forma que pertenezcan a una recta paralela a la rampa,

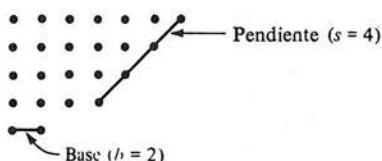


Figura 14.2

tal como se indica en la figura 14.3(a). La operación B mueve los puntos de la rampa de forma que pertenezcan a una recta paralela a la base, tal como se indica en la figura 14.3(b). Decimos que una operación es *permisible* si preserva la forma standard del grafo, es decir, si el nuevo grafo tiene también las partes desiguales colocadas en orden decreciente.

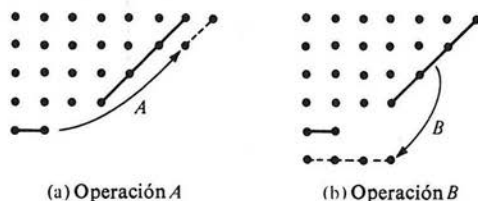


Figura 14.3

Si A es permisible obtenemos una nueva partición de n en partes desiguales, pero el número de partes es una unidad menor que antes de efectuar la operación A . Si B es permisible obtenemos una nueva partición en partes desiguales, pero el

número de partes de n es una unidad mayor que antes. Por consiguiente, si para cada partición de n exactamente una de las operaciones A o B es permisible, existe una correspondencia uno a uno entre particiones de n en partes desiguales en número par e impar, es decir $p_e(n) = p_o(n)$ para dicho n .

Para determinar cuando A y B son permisibles consideramos tres casos: (1) $b < s$; (2) $b = s$; (3) $b > s$.

Caso 1: Si $b < s$, entonces $b \leq s - 1$, luego la operación A es permisible, pero la B no porque destruye la forma estándar. (Ver figura 14.3.)

Caso 2: Si $b = s$, la operación B no es permisible ya que el grafo que resulta no se halla en forma estándar. La operación A es permisible excepto cuando la base y la rampa se intersecan como muestra la figura 14.4(a), en cuyo caso el nuevo grafo no se halla en forma estándar.

Caso 3: Si $b > s$, la operación A no es permisible, mientras que la B es permisible excepto si $b = s + 1$ y la base y la rampa se intersecan, como muestra la figura 14.4(b). En este caso el nuevo grafo tiene dos partes iguales.

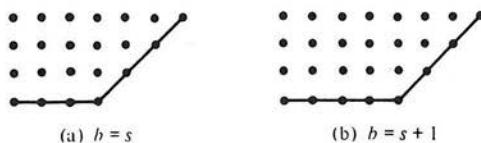


Figura 14.4 Ni A ni B son permisibles

Por consiguiente, exactamente una de las operaciones A o B es permisible, con las dos excepciones arriba indicadas. Consideremos en primer lugar el caso excepcional indicado en la figura 14.4(a) y supongamos que el grafo posee k filas. Entonces también $b = k$, luego el número n se obtiene por

$$n = k + (k + 1) + \cdots + (2k - 1) = \frac{3k^2 - k}{2} = \omega(k).$$

Para esta partición de n tenemos una partición extra en partes pares si k es par, y una partición extra en partes impares si k es impar, es decir

$$p_e(n) - p_o(n) = (-1)^k.$$

En el otro caso excepcional, indicado en la figura 14.4(b), existe un punto reticular adicional en cada fila o sea

$$n = \frac{3k^2 - k}{2} + k = \frac{3k^2 + k}{2} = \omega(-k)$$

y de nuevo $p_e(n) - p_o(n) = (-1)^k$. Esto termina la demostración de Franklin de la identidad de Euler.

14.6 FÓRMULA RECURSIVA DE EULER PARA $p(n)$

Teorema 14.4 Sea $p(0) = 1$ y definamos $p(n)$ igual a 0 si $n < 0$. Entonces, para $n \geq 1$, tenemos

$$(8) \quad p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) + \cdots = 0,$$

o bien, lo que es lo mismo,

$$p(n) = \sum_{k=1}^{\infty} (-1)^{k+1} \{p(n - \omega(k)) + p(n - \omega(-k))\}.$$

DEMOSTRACIÓN. Los teoremas 14.2 y 14.3 nos dan la identidad

$$\left(1 + \sum_{k=1}^{\infty} (-1)^k \{x^{\omega(k)} + x^{\omega(-k)}\}\right) \left(\sum_{m=0}^{\infty} p(m)x^m\right) = 1.$$

Si $n \geq 1$, el coeficiente de x^n de la derecha es 0, luego inmediatamente obtenemos (8) igualando coeficientes. $\square$

MacMahon utilizó esta fórmula recursiva para calcular $p(n)$ hasta $n = 200$. Damos algunos valores muestra de esta tabla.

$$\begin{aligned} p(1) &= 1 \\ p(5) &= 7 \\ p(10) &= 42 \\ p(15) &= 176 \\ p(20) &= 627 \end{aligned}$$

$$\begin{aligned}
 p(25) &= 1\,958 \\
 p(30) &= 5\,604 \\
 p(40) &= 37\,338 \\
 p(50) &= 204\,226 \\
 p(100) &= 190\,569\,292 \\
 p(200) &= 3\,972\,999\,029\,388
 \end{aligned}$$

Estos ejemplos indican que $p(n)$ crece muy rápidamente con n . El mayor valor de $p(n)$ calculado es $p(14\,031)$, y es un número con 127 dígitos. D. H. Lehmer [42] calculó este número para comprobar una conjetura de Ramanujan que afirma que $p(14\,031) \equiv 0 \pmod{11^4}$. Esta afirmación resultó correcta. Es obvio que para calcular este valor de $p(n)$ no se utilizó la fórmula dada en (8). En su lugar, Lehmer utilizó una fórmula asintótica de Rademacher [54] que implica

$$p(n) \sim \frac{e^{K\sqrt{n}}}{4n\sqrt{3}} \quad \text{cuando } n \rightarrow \infty,$$

en donde $K = \pi(2/3)^{1/2}$. Para $n = 200$ la cantidad de la derecha es aproximadamente 4×10^{12} que es notablemente próxima al valor de $p(200)$ dado en la tabla de MacMahon.

En la continuación de este volumen daremos una deducción de la fórmula asintótica de Rademacher de $p(n)$. La demostración requiere una preparación considerable en la teoría de las funciones modulares elípticas. En la sección siguiente se da una cota superior de $p(n)$ que involucra la exponencial $e^{K\sqrt{n}}$ y que se puede obtener con un esfuerzo relativamente pequeño.

14.7 UNA COTA SUPERIOR PARA $p(n)$

Teorema 14.5 Si $n \geq 1$, tenemos $p(n) < e^{K\sqrt{n}}$, en donde $K = \pi(2/3)^{1/2}$.

DEMOSTRACIÓN. Sea

$$F(x) = \prod_{n=1}^{\infty} (1 - x^n)^{-1} = 1 + \sum_{k=1}^{\infty} p(k)x^k,$$

y restrinjamos x al intervalo $0 < x < 1$. Entonces tenemos $p(n)x^n < F(x)$, de donde obtenemos $\log p(n) + n \log x < \log F(x)$, luego

$$(9) \quad \log p(n) < \log F(x) + n \log \frac{1}{x}.$$

Determinamos mayorantes de los términos $\log F(x)$ y de $n \log (1/x)$ separadamente. Primero escribimos

$$\begin{aligned} \log F(x) &= -\log \prod_{n=1}^{\infty} (1 - x^n) = -\sum_{n=1}^{\infty} \log(1 - x^n) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{x^{mn}}{m} \\ &= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{n=1}^{\infty} (x^m)^n = \sum_{m=1}^{\infty} \frac{1}{m} \frac{x^m}{1 - x^m}. \end{aligned}$$

Dado que tenemos

$$\frac{1 - x^m}{1 - x} = 1 + x + x^2 + \cdots + x^{m-1},$$

y que $0 < x < 1$, podemos escribir

$$mx^{m-1} < \frac{1 - x^m}{1 - x} < m,$$

y por tanto

$$\frac{m(1 - x)}{x} < \frac{1 - x^m}{x^m} < \frac{m(1 - x)}{x^m}.$$

Si invertimos y dividimos por m obtenemos

$$\frac{1}{m^2} \frac{x^m}{1 - x} \leq \frac{1}{m} \frac{x^m}{1 - x^m} \leq \frac{1}{m^2} \frac{x}{1 - x}.$$

Sumando respecto de m obtenemos

$$\log F(x) = \sum_{m=1}^{\infty} \frac{1}{m} \frac{x^m}{1 - x^m} \leq \frac{x}{1 - x} \sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6} \frac{x}{1 - x} = \frac{\pi^2}{6t},$$

en donde

$$t = \frac{1-x}{x}.$$

Obsérvese que t varía de ∞ a 0 positivamente cuando x varía de 0 a 1.

Ahora mayoramos el término $n \log(1/x)$. Para $t > 0$ tenemos $\log(1+t) < t$. Pero

$$1+t = 1 + \frac{1-x}{x} = \frac{1}{x}, \quad \text{luego} \quad \log \frac{1}{x} < t.$$

Ahora bien

$$(10) \quad \log p(n) < \log F(x) + n \log \frac{1}{x} < \frac{\pi^2}{6t} + nt.$$

El mínimo de $(\pi^2/6t) + nt$ se obtiene cuando ambos términos son iguales, esto es, cuando $\pi^2/(6t) = nt$, o bien $t = \pi/\sqrt{6n}$. Para este valor de t tenemos

$$\log p(n) < 2nt = 2n\pi/\sqrt{6n} = K\sqrt{n}$$

luego $p(n) < e^{K\sqrt{n}}$, como asegurábamos. □

Nota. J. H. van Lint [48] demostró que con un poco más de esfuerzo podemos obtener la desigualdad más precisa

$$(11) \quad p(n) < \frac{\pi e^{K\sqrt{n}}}{\sqrt{6(n-1)}} \quad \text{para } n > 1.$$

Como $p(k) \geq p(n)$ si $k \geq n$, tenemos, si $n > 1$,

$$F(x) > \sum_{k=n}^{\infty} p(k)x^k \geq p(n) \sum_{k=n}^{\infty} x^k = \frac{p(n)x^n}{1-x}.$$

Tomando logaritmos obtenemos, en vez de (9), la desigualdad

$$\log p(n) < \log F(x) + n \log \frac{1}{x} + \log(1-x).$$

Pero, al ser $1 - x = tx$, tenemos $\log(1 - x) = \log t - \log(1/x)$, luego (10) se puede substituir por

$$(12) \quad \log p(n) < \frac{\pi^2}{6t} + (n-1)t + \log t.$$

Un cálculo fácil con derivadas prueba que la función

$$f(t) = \frac{\pi^2}{6t} + (n-1)t + \log t$$

tiene un mínimo en

$$t = \frac{-1 + \sqrt{1 + [4(n-1)\pi^2/6]}}{2(n-1)}.$$

Utilizando este valor de t en (12) y despreciando términos insignificantes obtenemos (11).

14.8 IDENTIDAD DEL TRIPLE PRODUCTO DE JACOBI

Esta sección describe una identidad famosa de la teoría de la función zeta debida a Jacobi. El teorema de los números pentagonales de Euler y muchas otras identidades con particiones se obtienen como casos especiales de la fórmula de Jacobi.

Teorema 14.6 Identidad del triple producto de Jacobi. *Para x y z complejos con $|x| < 1$ y $z \neq 0$ tenemos*

$$(13) \quad \prod_{n=1}^{\infty} (1 - x^{2n})(1 + x^{2n-1}z^2)(1 + x^{2n-1}z^{-2}) = \sum_{m=-\infty}^{\infty} x^{m^2} z^{2m}.$$

DEMOSTRACIÓN. La restricción a $|x| < 1$ nos asegura la convergencia absoluta de cada uno de los productos $\prod (1 - x^{2n})$, $\prod (1 + x^{2n-1}z^2)$, $\prod (1 + x^{2n-1}z^{-2})$, y de la serie de (13). Además, para cada x con $|x| < 1$, la serie y los productos convergen uniformemente sobre subconjuntos compactos del z -plano siempre que no

contengan a $z = 0$, por lo que cada miembro de (13) es una función analítica de z para $z \neq 0$. Para $z \neq 0$ fijo, la serie y los productos también convergen uniformemente para $|x| \leq r < 1$, luego representan funciones analíticas de x en el disco $|x| < 1$.

Para probar (13) fijamos x y definimos $F(z)$ para $z \neq 0$ por la ecuación

$$(14) \quad F(z) = \prod_{n=1}^{\infty} (1 + x^{2n-1}z^2)(1 + x^{2n-1}z^{-2}).$$

En primer lugar vemos que F satisface la ecuación funcional

$$(15) \quad xz^2F(xz) = F(z).$$

De (14) obtenemos

$$\begin{aligned} F(xz) &= \prod_{n=1}^{\infty} (1 + x^{2n+1}z^2)(1 + x^{2n-3}z^{-2}) \\ &= \prod_{m=2}^{\infty} (1 + x^{2m-1}z^2) \prod_{r=0}^{\infty} (1 + x^{2r-1}z^{-2}). \end{aligned}$$

Puesto que $xz^2 = (1 + xz^2)/(1 + x^{-1}z^{-2})$, la multiplicación de la última ecuación por xz^2 da (15).

Ahora sea $G(z)$ el miembro de la izquierda de (13), o sea

$$(16) \quad G(z) = F(z) \prod_{n=1}^{\infty} (1 - x^{2n}).$$

Entonces $G(z)$ también satisface la ecuación funcional (15). Además, $G(z)$ es una función par de z que es analítica en todo $z \neq 0$, luego admite un desarrollo de Laurent de la forma

$$(17) \quad G(z) = \sum_{m=-\infty}^{\infty} a_m z^{2m}$$

en donde $a_{-m} = a_m$ ya que $G(z) = G(z^{-1})$. (Los coeficientes a_m dependen de x .) Utilizando la ecuación funcional (15) en (17) obtenemos que los coeficientes satisfacen la fórmula recursiva

$$a_m = x^{2m-1} a_{m-1}$$

que, al iterarla, nos da

$$a_m = a_0 x^{m^2} \quad \text{para todo } m \geq 0$$

ya que $1 + 3 + \dots + (2m-1) = m^2$. Este resultado se verifica también para $m < 0$. Luego (17) se transforma en

$$(18) \quad G_x(z) = a_0(x) \sum_{m=-\infty}^{\infty} x^{m^2} z^{2m},$$

en donde hemos escrito $G_x(z)$ en vez de $G(z)$ y $a_0(x)$ en vez de a_0 para indicar la dependencia de x . Observamos que (18) implica que $a_0(x) \rightarrow 1$ cuando $x \rightarrow 0$. Para terminar la demostración debemos probar que $a_0(x) = 1$ para todo x .

Si hacemos $z = e^{\pi i/4}$ en (18) obtenemos

$$(19) \quad \frac{G_x(e^{\pi i/4})}{a_0(x)} = \sum_{m=-\infty}^{\infty} x^{m^2} i^m = \sum_{n=-\infty}^{\infty} (-1)^n x^{(2n)^2}$$

ya que $i^m = -i^{-m}$ si m es impar. De (18) deducimos que la serie de la derecha de 19 es $G_{x^4}(i)/a_0(x^4)$ de donde se sigue la identidad

$$(20) \quad \frac{G_x(e^{\pi i/4})}{a_0(x)} = \frac{G_{x^4}(i)}{a_0(x^4)}.$$

A continuación probamos que $G_x(e^{\pi i/4}) = G_{x^4}(i)$. En efecto, (14) y (16) nos dan

$$G_x(e^{\pi i/4}) = \prod_{n=1}^{\infty} (1 - x^{2n})(1 + x^{4n-2}).$$

Como cada número par es de la forma $4n$ o $4n-2$ tenemos

$$\prod_{n=1}^{\infty} (1 - x^{2n}) = \prod_{n=1}^{\infty} (1 - x^{4n})(1 - x^{4n-2})$$

luego

$$\begin{aligned} G_x(e^{\pi i/4}) &= \prod_{n=1}^{\infty} (1 - x^{4n})(1 - x^{4n-2})(1 + x^{4n-2}) = \prod_{n=1}^{\infty} (1 - x^{4n})(1 - x^{8n-4}) \\ &= \prod_{n=1}^{\infty} (1 - x^{8n})(1 - x^{8n-4})(1 - x^{8n-4}) = G_{x^4}(i). \end{aligned}$$

Por lo tanto (20) implica $a_0(x) = a_0(x^4)$. Si sustituimos x por $x^4, x^{16}, \dots$, obtenemos

$$a_0(x) = a_0(x^{4^k}) \quad \text{para } k = 1, 2, \dots$$

Pero $x^{4^k} \rightarrow 0$ cuando $k \rightarrow \infty$ y $a_0(x) \rightarrow 1$ cuando $x \rightarrow 0$, luego $a_0(x) = 1$ para todo x . Esto completa la demostración. $\square$

14.9 CONSECUENCIAS DE LA IDENTIDAD DE JACOBI

Si sustituimos x por x^a y z^2 por x^b en la identidad de Jacobi obtenemos

$$\prod_{n=1}^{\infty} (1 - x^{2na})(1 + x^{2na-a+b})(1 + x^{2na-a-b}) = \sum_{m=-\infty}^{\infty} x^{am^2+bm}.$$

Análogamente, si $z^2 = -x^b$ obtenemos

$$\prod_{n=1}^{\infty} (1 - x^{2na})(1 - x^{2na-a+b})(1 - x^{2na-a-b}) = \sum_{m=-\infty}^{\infty} (-1)^m x^{am^2+bm}.$$

Para obtener el teorema de los números pentagonales de Euler hacemos simplemente $a = 3/2$ y $b = 1/2$ en esta última igualdad

La fórmula de Jacobi conduce a otra fórmula importante para el cubo del producto de Euler.

Teorema 14.7 Si $|x| < 1$ tenemos

$$(21) \quad \prod_{n=1}^{\infty} (1 - x^n)^3 = \sum_{m=-\infty}^{\infty} (-1)^m m x^{(m^2+m)/2} = \sum_{m=0}^{\infty} (-1)^m (2m+1) x^{(m^2+m)/2}.$$

DEMOSTRACIÓN. Substituimos z^2 por $-xz$ en la identidad de Jacobi y obtenemos

$$\prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n}z)(1 - x^{2n-2}z^{-1}) = \sum_{m=0}^{\infty} (-1)^m x^{m^2+m} (z^m - z^{-m-1}).$$

Ahora reordenamos los términos de ambos miembros, utilizando las relaciones

$$\prod_{n=1}^{\infty} (1 - x^{2n-2}z^{-1}) = (1 - z^{-1}) \prod_{n=1}^{\infty} (1 - x^{2n}z^{-1})$$

y

$$z^m - z^{-m-1} = (1 - z^{-1})(1 + z^{-1} + z^{-2} + \dots + z^{-2m})z^m.$$

Anulando el factor $1 - z^{-1}$ obtenemos

$$\begin{aligned} \prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n}z)(1 - x^{2n}z^{-1}) \\ = \sum_{m=0}^{\infty} (-1)^m x^{m^2+m} z^m (1 + z^{-1} + z^{-2} + \dots + z^{-2m}). \end{aligned}$$

Si hacemos $z = 1$ y sustituimos x por $x^{1/2}$ obtenemos (21). □

14.10 DIFERENCIACIÓN LOGARÍTMICA DE FUNCIONES GENERADORAS

El teorema 14.4 da una fórmula recursiva de $p(n)$. Existen otros tipos de fórmulas recursivas de funciones aritméticas que se pueden obtener por medio de la diferenciación logarítmica de funciones generadoras. A continuación describimos este método.

Sea A un conjunto de números positivos dado, y sea $f(n)$ una función aritmética. Suponemos que el producto

$$F_A(x) = \prod_{n \in A} (1 - x^n)^{-f(n)/n}$$

y la serie

$$G_A(x) = \sum_{n \in A} \frac{f(n)}{n} x^n$$

convergen absolutamente para $|x| < 1$ y representan funciones analíticas en el disco unidad $|x| < 1$. El logaritmo del producto viene expresado por

$$\log F_A(x) = - \sum_{n \in A} \frac{f(n)}{n} \log(1 - x^n) = \sum_{n \in A} \frac{f(n)}{n} \sum_{m=1}^{\infty} \frac{x^{mn}}{m} = \sum_{m=1}^{\infty} \frac{1}{m} G_A(x^m).$$

Diferenciando y multiplicando por x obtenemos

$$x \frac{F'_A(x)}{F_A(x)} = \sum_{m=1}^{\infty} G'_A(x^m) x^m = \sum_{m=1}^{\infty} \sum_{n \in A} f(n) x^{mn} = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi_A(n) f(n) x^{mn},$$

en donde χ_A es la función característica del conjunto A ,

$$\chi_A(n) = \begin{cases} 1 & \text{si } n \in A, \\ 0 & \text{si } n \notin A. \end{cases}$$

Agrupando los términos con $mn = k$ obtenemos

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi_A(n) f(n) x^{mn} = \sum_{k=1}^{\infty} f_A(k) x^k,$$

en donde

$$f_A(k) = \sum_{d|k} \chi_A(d) f(d) = \sum_{\substack{d|k \\ d \in A}} f(d).$$

Por consiguiente tenemos la siguiente identidad,

$$(22) \quad xF'_A(x) = F_A(x) \sum_{k=1}^{\infty} f_A(k)x^k.$$

Ahora escribimos el producto $F_A(x)$ como una serie de potencias

$$F_A(x) = \sum_{n=0}^{\infty} p_{A,f}(n)x^n, \text{ en donde } p_{A,f}(0) = 1,$$

e igualamos los coeficientes de x^n de (22) para obtener la fórmula recursiva (24) en el teorema siguiente.

Teorema 14.8 *Para un conjunto dado A y una función aritmética f , los números $p_{A,f}(n)$ definidos por la ecuación*

$$(23) \quad \prod_{n \in A} (1 - x^n)^{-f(n)/n} = 1 + \sum_{n=1}^{\infty} p_{A,f}(n)x^n$$

satisfacen la fórmula recursiva

$$(24) \quad np_{A,f}(n) = \sum_{k=1}^n f_A(k)p_{A,f}(n-k),$$

en donde $p_{A,f}(0) = 1$ y

$$f_A(k) = \sum_{\substack{d|k \\ d \in A}} f(d).$$

EJEMPLO 1 Sea A el conjunto de todos los enteros positivos. Si $f(n) = n$, entonces $p_{A,f}(n) = p(n)$, que es la función de partición no restringida, y $f_A(k) = \sigma(k)$, que es la suma de los divisores de k . La ecuación (24) da

$$np(n) = \sum_{k=1}^n \sigma(k)p(n-k),$$

que es una relación notable que conecta una función de la teoría multiplicativa de números con una de la teoría aditiva de números.

EJEMPLO 2 Tomamos A igual al del ejemplo 1, pero $f(n) = -n$. Entonces los coeficientes de (23) se hallan determinados por el teorema de los números pentagonales de Euler y la fórmula recursiva (24) da

$$(25) \quad np_{A,f}(n) = - \sum_{k=1}^n \sigma(k)p_{A,f}(n-k) = -\sigma(n) - \sum_{k=1}^{n-1} p_{A,f}(k)\sigma(n-k),$$

en donde

$$p_{A,f}(n) = \begin{cases} (-1)^m & \text{si } n \text{ es un número pentagonal } \omega(m) \text{ o } \omega(-m) \\ 0 & \text{si } n \text{ no es un número pentagonal.} \end{cases}$$

La ecuación (25) también se puede escribir como sigue:

$$\begin{aligned} \sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) - \dots \\ = \begin{cases} (-1)^{m-1}\omega(m) & \text{si } n = \omega(m), \\ (-1)^{m-1}\omega(-m) & \text{si } n = \omega(-m), \\ 0 & \text{en otro caso.} \end{cases} \end{aligned}$$

La suma de la izquierda termina cuando el término $\sigma(k)$ tiene $k \leq 1$. Para ilustrarlo, cuando $n = 6$ y $n = 7$, esto nos da las relaciones

$$\begin{aligned} \sigma(6) &= \sigma(5) + \sigma(4) - \sigma(1), \\ \sigma(7) &= \sigma(6) + \sigma(5) - \sigma(2) - 7. \end{aligned}$$

14.11 LAS IDENTIDADES DE PARTICIÓN DE RAMANUJAN

Examinando la tabla de Macmahon de la función de partición, Ramanujan llegó a descubrir ciertas propiedades de divisibilidad sorprendentes de $p(n)$. Por ejemplo, probó que

$$(26) \quad p(5m+4) \equiv 0 \pmod{5},$$

$$(27) \quad p(7m+5) \equiv 0 \pmod{7},$$

$$(28) \quad p(11m+6) \equiv 0 \pmod{11}.$$

En relación con estos descubrimientos estableció también sin demostración dos identidades notables

$$(29) \quad \sum_{m=0}^{\infty} p(5m+4)x^m = 5 \frac{\varphi(x^5)^5}{\varphi(x)^6},$$

y

$$(30) \quad \sum_{m=0}^{\infty} p(7m+5)x^m = 7 \frac{\varphi(x^7)^3}{\varphi(x)^4} + 49x \frac{\varphi(x^7)^7}{\varphi(x)^8},$$

en donde

$$\varphi(x) = \prod_{n=1}^{\infty} (1 - x^n).$$

Dado que las funciones de la derecha de (29) y (30) admiten desarrollos en serie de potencias con coeficientes enteros, las identidades de Ramanujan implican de forma inmediata las congruencias (26) y (27).

Las demostraciones de (29) y (30), basadas en la teoría de las funciones modulares, fueron establecidas por Darling, Mordell, Rademacher, Zuckerman, y otros. Demostraciones posteriores, independientes de la teoría de las funciones modulares, fueron establecidas por Kruyswijk [36] y posteriormente por Kolberg. El método de Kolberg no sólo da las identidades de Ramanujan sino muchas otras. La demostración de Kruyswijk de (29) se establece en los ejercicios 11-15.

Ejercicios del capítulo 14

1. Sea A un conjunto no vacío de números positivos.

(a) Probar que el producto

$$\prod_{m \in A} (1 - x^m)^{-1}$$

es la función generadora del número de particiones de n en partes pertenecientes al conjunto A .

- (b) Describir la función de partición generada por el producto

$$\prod_{m \in A} (1 + x^m).$$

En particular, describir la función de partición generada por el producto finito

$$\prod_{m=1}^k (1 + x^m).$$

2. Si $|x| < 1$, probar que

$$\prod_{m=1}^{\infty} (1 + x^m) = \prod_{m=1}^{\infty} (1 - x^{2m-1})^{-1},$$

y deducir que el número de particiones de n en partes desiguales es igual al número de particiones de n en partes impares.

3. Para complejos x y z con $|x| < 1$, consideramos

$$f(x, z) = \prod_{m=1}^{\infty} (1 - x^m z).$$

- (a) Probar que, para cada z fijo, el producto es una función analítica de x en el disco $|x| < 1$, y que, para cada x fijo con $|x| < 1$, el producto es una función entera de z .
 (b) Definimos los números $a_n(x)$ por la ecuación

$$f(x, z) = \sum_{n=0}^{\infty} a_n(x) z^n.$$

Probar que $f(x, z) = (1 - zx)f(x, zx)$ y utilizarlo para demostrar que los coeficientes satisfacen la fórmula recursiva

$$a_n(x) = a_n(x)x^n - a_{n-1}(x)x^n.$$

- (c) De la parte (b) deducir que $a_n(x) = (-1)^n x^{n(n+1)/2} / P_n(x)$, en donde

$$P_n(x) = \prod_{r=1}^n (1 - x^r).$$

Este resultado prueba la siguiente identidad para $|x| < 1$ y z arbitrario:

$$\prod_{m=1}^{\infty} (1 - x^m z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{P_n(x)} x^{n(n+1)/2} z^n.$$

4. Utilizar un procedimiento análogo al del ejercicio 3 para demostrar que, si $|x| < 1$ y $|z| < 1$ tenemos

$$\prod_{m=1}^{\infty} (1 - x^m z)^{-1} = \sum_{n=0}^{\infty} \frac{z^n}{P_n(x)}$$

en donde $P_n(x) = \prod_{r=1}^n (1 - x^r)$.

5. Si $x \neq 1$, sea $Q_0(x) = 1$ y, para $n \geq 1$, definamos

$$Q_n(x) = \prod_{r=1}^n \frac{1 - x^{2r}}{1 - x^{2r-1}}.$$

- (a) Deducir las siguientes identidades finitas de Shanks:

$$\sum_{m=1}^{2n} x^{m(m-1)/2} = \sum_{s=0}^{n-1} \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)},$$

$$\sum_{m=1}^{2n+1} x^{m(m-1)/2} = \sum_{s=0}^n \frac{Q_n(x)}{Q_s(x)} x^{s(2n+1)}.$$

- (b) Utilizar las identidades de Shanks para deducir el teorema de los números triangulares de Gauss:

$$\sum_{m=1}^{\infty} x^{m(m-1)/2} = \prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^{2n-1}} \quad \text{para } |x| < 1.$$

6. La identidad que sigue es válida para $|x| < 1$:

$$\sum_{m=-\infty}^{\infty} x^{m(m+1)/2} = \prod_{n=1}^{\infty} (1+x^{n-1})(1-x^{2n}).$$

- (a) Deducirla de las identidades de los ejercicios 2 y 5(b).
 (b) Deducirla de la identidad del triple producto de Jacobi.
7. Probar que las siguientes identidades, válidas para $|x| < 1$, son consecuencias de la identidad del triple producto de Jacobi:

$$(a) \prod_{n=1}^{\infty} (1-x^{5n})(1-x^{5n-1})(1-x^{5n-4}) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+3)/2}.$$

$$(b) \prod_{n=1}^{\infty} (1-x^{5n})(1-x^{5n-2})(1-x^{5n-3}) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(5m+1)/2}.$$

8. Probar que la fórmula recursiva

$$np(n) = \sum_{k=1}^n \sigma(k)p(n-k),$$

obtenida en la sección 14.10 se puede poner en la forma

$$np(n) = \sum_{m=1}^n \sum_{k \leq n/m} mp(n-km).$$

9. Suponemos que cada entero positivo k se escribe en $g(k)$ colores distintos, en donde $g(k)$ es un entero positivo. Sea $p_g(n)$ el número de particiones de n en las que cada parte k aparece a lo sumo en $g(k)$ colores diferentes. Cuando $g(k) = 1$ para todo k , obtenemos la función de partición no restringida $p(n)$. Buscar un producto infinito que genere $p_g(n)$ y probar que existe una función aritmética f (que depende de g) tal que

$$np_g(n) = \sum_{k=1}^n f(k)p_g(n-k).$$

10. La notación es la referente a la sección 14.10. Resolviendo la ecuación diferencial de primer orden en (22) probar que, si $|x| < 1$, tenemos

$$\prod_{n \in A} (1 - x^n)^{-f(n)/n} = \exp \left\{ \int_0^x \frac{H(t)}{t} dt \right\},$$

en donde

$$H(x) = \sum_{k=1}^{\infty} f_A(k)x^k \quad \text{y} \quad f_A(k) = \sum_{\substack{d|k \\ d \in A}} f(d).$$

Deducir que

$$\prod_{n=1}^{\infty} (1 - x^n)^{\mu(n)/n} = e^{-x} \quad \text{para } |x| < 1,$$

en donde $\mu(n)$ es la función de Möbius.

Los ejercicios que siguen proporcionan una demostración de la identidad de partición de Ramanujan

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5 \frac{\varphi(x^5)^5}{\varphi(x)^6}, \quad \text{en donde } \varphi(x) = \prod_{n=1}^{\infty} (1 - x^n),$$

por un método de Kruyswijk que no requiere la teoría de las funciones modulares.

11. (a) Sea $\varepsilon = e^{2\pi i/k}$, en donde $k \geq 1$ probar que, para todo x , tenemos

$$\prod_{h=1}^k (1 - x\varepsilon^h) = 1 - x^k.$$

- (b) En general, si $(n, k) = d$, probar que

$$\prod_{h=1}^k (1 - x\varepsilon^{nh}) = (1 - x^{k/d})^d,$$

y deducir que

$$\prod_{h=1}^k (1 - x^n e^{2\pi i n h/k}) = \begin{cases} 1 - x^{nk} & \text{si } (n, k) = 1, \\ (1 - x^n)^k & \text{si } k|n. \end{cases}$$

12. (a) Utilizar el ejercicio 11(b) para probar que, para q primo y $|x| < 1$, tenemos

$$\prod_{n=1}^{\infty} \prod_{h=1}^q (1 - x^n e^{2\pi i n h / q}) = \frac{\varphi(x^q)^{q+1}}{\varphi(x^{q^2})}.$$

(b) Deducir la identidad

$$\sum_{m=0}^{\infty} p(m)x^m = \frac{\varphi(x^{25})}{\varphi(x^5)^6} \prod_{h=1}^4 \prod_{n=1}^{\infty} (1 - x^n e^{2\pi i n h / 5}).$$

13. Se dice que una serie de potencias de la forma

$$\sum_{n=0}^{\infty} a(n)x^{qn+r}$$

es de *tipo* $r \bmod q$, si q es primo y si $0 \leq r < q$.

(a) Utilizar el teorema de los números pentagonales de Euler para demostrar que $\varphi(x)$ es una suma de tres series de potencias,

$$\varphi(x) = \prod_{n=1}^{\infty} (1 - x^n) = I_0 + I_1 + I_2,$$

en donde I_k designa una serie de potencias de tipo $k \bmod 5$.

(b) Sea $\alpha = e^{2\pi i / 5}$ y pruébese que

$$\prod_{h=1}^4 \prod_{n=1}^{\infty} (1 - x^n \alpha^{nh}) = \prod_{h=1}^4 (I_0 + I_1 \alpha^h + I_2 \alpha^{2h}).$$

(c) Utilizar el ejercicio 12(b) para probar que

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = V_4 \frac{\varphi(x^{25})}{\varphi(x^5)^6},$$

en donde V_4 es la serie de potencias de tipo 4 mod 5 obtenida del producto de la parte (b).

14. (a) Utilizar el teorema 14.7 para probar que el cubo del producto de Euler es la suma de tres series de potencias,

$$\varphi(x)^3 = W_0 + W_1 + W_3,$$

en donde W_k indica una serie de potencias de tipo $k \bmod 5$.

(b) Utilizar la identidad $W_0 + W_1 + W_3 = (I_0 + I_1 + I_2)^3$ para probar que la serie de potencias del ejercicio 13(a) satisface la relación

$$I_0 I_2 = -I_1^2.$$

(c) Probar que $I_1 = -x\varphi(x^{25})$.

15. Observar que el producto $\prod_{h=1}^4 (I_0 I_1 \alpha^h + I_2 \alpha^{2h})$ es un polinomio homogéneo en I_0, I_1, I_2 de grado 4, por lo que los términos que contribuyen a la serie de tipo 4 mod 5 provienen de los términos $I_1^4, I_0 I_1^2 I_2$ e $I_0^2 I_2^2$.

(a) Utilizar el ejercicio 14(c) para demostrar que existe una constante c tal que

$$V_4 = cI_1^4,$$

en donde V_4 es la serie de potencias del ejercicio 13(c), y deducir que

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4} = cx^4 \frac{\varphi(x^{25})^5}{\varphi(x^5)^6}.$$

(b) Probar que $c = 5$ y deducir la identidad de Ramanujan

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5 \frac{\varphi(x^5)^5}{\varphi(x)^6}.$$

Bibliografía

MR indica una referencia a *Mathematical Reviews*.

1. Apostol, Tom M. (1970) Euler's φ -function and separable Gauss sums. *Proc. Amer. Math. Soc.*, 24: 482-485; MR 41, # 1661.
2. Apostol, Tom M. (1976) *Análisis matemático*, 2.^a edición. Edit. Reverté, S. A., Barcelona.
3. Ayoub, Raymond G. (1963) *An Introduction to the Analytic Theory of Numbers*. Mathematical Surveys, No. 10. Providence, R. I.: American Mathematical Society.
4. Bell, E. T. (1915) An arithmetical theory of certain numerical functions. *University of Washington Publ. in Math. and Phys. Sci.*, No. 1, Vol. 1: 1-44.
5. Borévič, Z. I., Šafarevič, I. R. (1966) *Teoría de Números*, Moscú (en ruso), 1.^a ed., 1964, 2.^a ed., 1972; *Number Theory*, New York (traducción inglesa de la 1.^a ed., rusa), Academic Press, 1965; *Théorie des Nombres* (traducción francesa de la 1.^a ed. rusa), Gauthiers Villars.
- 5.a Borozdkin, K. G. (1956) K voprosu o postoyanni I. M. Vinogradova. *Trudy tret'ego vsesoiuznogo matematičeskogo s'ezda*, Vol. I, Moskva [Russian].
6. Buhštab, A. A. (1965) New results in the investigation of the Goldbach-Euler problem and the problem of prime pairs. [Russian]. *Dokl. Akad. Nauk SSSR*, 162: 735-738; MR 31, # 2226. [English translation: (1965) *Soviet Math. Dokl.* 6: 729-732.]
7. Chandrasekharan, Komaravolu (1958) *Introduction to Analytic Number Theory*. Die Grundlehren der Mathematischen Wissenschaften, Band 148. New York: Springer-Verlag.
8. Chandrasekharan, Komaravolu (1970) *Aritmetical Functions*. Die Grundlehren der Mathematischen Wissenschaften, Band 167. New York: Springer-Verlag.
9. Chebyshev, P. L. Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée. (a) (1851) *Mem. Ac. Sc. St. Pétersbourg*, 6: 141-157. (b) (1852) *Jour. de Math* (1) 17: 341-365. [Oeuvres, 1: 27-48.]
10. Chen, Jing-run (1966) On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Kexue Tongbao* (Foreign Lang. Ed.), 17: 385-386; MR 34, # 7483.
11. Clarkson, James A. (1966) On the series of prime reciprocals. *Proc. Amer. Math. Soc.*, 17: 541; MR 32, # 5573.
12. Davenport, Harold (1967) *Multiplicative Number Theory*. Lectures in Advanced Mathematics, No. 1. Chicago: Markham Publishing Co.
13. Dickson, Leonard Eugene (1919) *History of the Theory of Numbers*. (3 volumes). Washington,

- D. C.: Carnegie Institution of Washington. Reprinted by Chelsea Publishing Co., New York, 1966.
14. Dickson, Leonard Eugene (1930) *Studies in the Theory of Numbers*. Chicago: The University of Chicago Press.
 15. Dirichlet, P. G. Lejeune (1837) Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendliche viele Primzahlen enthält. *Abhand. Ak. Wiss. Berlin*: 45-81. [*Werke*, 1: 315-342.]
 16. Dirichlet, P. G. Lejeune (1840) Ueber eine Eigenschaft der quadratischen Formen. *Bericht Ak. Wiss. Berlin*: 49-52. [*Werke*, 1: 497-502.]
 17. Edwards, H. M. (1974) *Riemann's Zeta Function*. New York and London: Academic Press.
 18. Ellison, W. J. (1971) Waring's problem. *Amer. Math. Monthly*, 78: 10-36.
 19. Erdős, Paul (1949) On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Nat. Acad. Sci. U.S.A.*, 35: 374-384; MR 10, 595.
 20. Euler, Leonhard (1737) Variarum observationes circa series infinitas. *Commentarii Academiae Scientiarum Imperialis Petropolitane*, 9: 160-188. [*Opera Omnia* (1), 14; 216-244.]
 21. Euler, Leonhard (1748) *Introductio in Analysin Infinitorum*, Vol. 1. Lausanne: Bousquet. [*Opera Omnia* (1), 8.]
 22. Franklin, F. (1881) Sur le développement du produit infini $(1-x)(1-x^2)(1-x^3)(1-x^4)\dots$. *Comptes Rendus Acad. Sci. (Paris)*, 92: 448-450.
 23. Gauss, C. F. (1801) *Disquisitiones Arithmeticae*. Lipsiae. [English translation: Arthur A. Clarke (1966) New Haven: Yale University Press.
 24. Gauss, C. F. (1849) Carta a Encke, con fecha 24 December. [*Werke*, Vol. II, 444-447.]
 25. Gerstenhaber, Murray (1963) The 152nd proof of the law of quadratic reciprocity. *Amer. Math. Monthly*, 70: 397-398; MR 27, # 100.
 26. Goldbach, C. (1742) Carta a Euler, con fecha 7 June.
 27. Grosswald, Emil (1966) *Topics from the Theory of Numbers*. New York: The Macmillan Co.
 28. Hadamard, J. (1896) Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24: 199-220.
 29. Hagi, Peter, Jr. (1937) A lower bound for the set of odd perfect numbers. *Math. Comp.*, 27: 951-953; MR 48, # 3854.
 30. Hardy, G. H. (1940) *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*. Cambridge: The University Press.
 31. Hardy, G. H. and Wright, E. M. (1960) *An Introduction to the Theory of Numbers*, 4th ed. Oxford: Clarendon Press.
 32. Hemer, Ove (1954) Notes on the Diophantine equation $y^2 - k = x^3$. *Ark. Mat.*, 3: 67-77; MR 15, 776.
 33. Ingham, A. E. (1932) *The Distribution of Prime Numbers*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 30. Cambridge: The University Press.
 34. Jacobi, C. G. J. (1829) *Fundamenta Nova Theoriae Functionum Ellipticarum* [*Gesammelte Werke*, Band I, 49-239.]
 35. Karatsuba, A. (1979) *Fundamentos de la teoría analítica de los números* (traducción española de la 1.ª ed. rusa), Ed. MIR, Moscú.
 - 35.a Kolesnik, G. A. (1969) An improvement of the remainder term in the divisor problem. (Russian). *Mat. Zametki*, 6: 545-554; MR 41, # 1659. [English translation: (1969), *Math. Notes*, 6: 784-791.]
 36. Kruyswijk, D. (1950) On some well-known properties of the partition function $p(n)$ and Euler's infinite product. *Nieuw Arch. Wisk.*, (2) 23: 97-107; MR 11, 715.
 37. Landau, E. (1909) *Handbuch der Lehre von der Verteilung der Primzahlen*. Leipzig: Teubner. Reprinted by Chelsea, 1953.
 38. Landau, E. (1927) *Vorlesungen über Zahlentheorie* (3 volumes). Leipzig: Hirzel. Reprinted

- by Chelsea, 1947.
39. Leech, J. (1957) Note on the distribution of prime numbers. *J. London Math. Soc.*, 32: 56-58; *MR* 18, 642.
 40. Legendre, A. M. (1798) *Essai sur la Theorie des Nombres*. Paris: Duprat.
 41. Lehmer, D. H. (1959) On the exact number of primes less a given limit. *Illinois J. Math.*, 3: 381-388; *MR* 21, # 5613.
 42. Lehmer, D. H. (1936) On a conjecture of Ramanujan. *J. London Math. Soc.*, 11: 114-118.
 43. Lehmer, D. N. (1914) List of prime numbers from 1 to 10, 006, 721. Washington, D.C.: Carnegie Institution of Washington, Publ. No. 165.
 44. LeVeque, W. J. (1956) *Topics in Number Theory* (2 volumes). Reading, Mass.: Addison-Wesley Publishing Co.
 45. LeVeque, W. J. (1974) *Reviews in Number Theory* (6 volumes). Providence, RI: American Mathematical Society.
 46. Levinson, N. (1969) A motivated account of an elementary proof of the prime number theorem. *Amer. Math. Monthly*, 76: 225-245; *MR* 39 # 2712.
 47. Levinson, Norman (1974) More than one third of zeros of Riemann's zeta-function are on $\sigma = 1/2$. *Advances Math.*, 13: 383-436.
 48. van Lint, Jacobus Hendricus (1974) *Combinatorial Theory Seminar* (Eindhoven University of Technology), Lecture Notes in Mathematics 382. Springer-Verlag, Chapter 4.
 49. Littlewood, J. E. (1914) Sur la distribution des nombres premiers. *Comptes Rendus Acad. Sci. (Paris)*, 158: 1869-1872.
 50. Mills, W. H. (1947) A prime-representing function. *Bull. Amer. Math. Soc.*, 53: 604; *MR* 8, 567.
 51. Nevanlinna, V. (1962) Über den elementaren Beweis des Primzahlsatzes. *Soc. Sci. Fenn. Comment. Phys.-Math.*, 27 No. 3, 8 pp.; *MR* 26, # 2416.
 52. Niven, I. and Zuckerman, H. S. (1972) *An Introduction to the Theory of Numbers*, 3rd ed. New York: John Wiley and Sons, Inc.
 53. Prachar, Karl (1957) *Primzahlverteilung*. Die Grundlehren der Mathematischen Wissenschaften, Band 91. Berlin-Göttingen-Heidelberg: Springer-Verlag.
 54. Rademacher, Hans (1937) On the partition function $p(n)$. *Proc. London Math. Soc.*, 43: 241-254.
 55. Rademacher, Hans (1964) *Lectures on Elementary Number Theory*. New York: Blaisdell Publishing Co.
 56. Rademacher, Hans (1973) *Topics in Analytic Number Theory*. Die Grundlehren der Mathematischen Wissenschaften, Band 169. New York-Heidelberg-Berlin: Springer-Verlag.
 57. Rényi, A. (1948) On the representation of an even number as the sum of a single prime and a single almost-prime number. (Russian). *Izv. Akad. Nauk SSSR Ser. Mat.*, 12: 57-78; *MR* 9, 413. [English translation: (1962) *Amer. Math. Soc. Transl.* 19 (2): 299-321.]
 58. Riemann, B. (1859) Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsber. Akad. Berlin*, 671-680.
 59. Robinson, R. M. (1958) A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers. *Proc. Amer. Math. Soc.*, 9: 673-681; *MR* 20, # 3097.
 60. Rosser, J. Barkley, and Schoenfeld, Lowell (1962) Approximate formulas for some functions of prime number theory. *Illinois J. Math.*, 6: 69-94; *MR* 25, # 1139.
 61. Schnirelmann, L. (1930) On additive properties of numbers. (Russian). *Izv. Donskovo Politechn. Inst. (Nowotscherkask)*, 14 (2-3): 3-28.
 62. Selberg, Atle (1949) An elementary proof of the prime number theorem. *Ann. of Math.*, 50: 305-313; *MR* 10, 595.
 63. Shanks, Daniel (1951) A short proof of an identity of Euler. *Proc. Amer. Math. Soc.*, 2: 747-749; *MR* 13, 321.
 64. Shapiro, Harold N. (1950) On the number of primes less than or equal x . *Proc. Amer. Math. Soc.*, 1: 346-348; *MR* 12, 80.

65. Shapiro, Harold N. (1952) On primes in arithmetic progression II. *Ann. of Math.* 52: 231-243; MR 12, 81.
66. Shen, Mok-Kong (1964) On checking the Goldbach conjecture. *Nordisk Tidskr. Informations-Behandling*, 4: 243-245; MR 30, # 3051.
67. Sierpinski, Waclaw (1964) *Elementary Theory of Numbers*. Translated from Polish by A. Hulanicki. Monografie Matematyczne Tom 42. Warsaw: Państwowe Wydawnictwo Naukowe.
68. Tatzuwa, Tikao, and Iseki, Kaneshiro (1951) On Selberg's elementary proof of the prime number theorem. *Proc. Japan Acad.*, 27: 340-342; MR 13, 725.
69. Titchmarsh, E. C. (1951) *The Theory of the Riemann Zeta Function*. Oxford: Clarendon Press.
70. Uspensky, J. V., and Heaslett, M. A. (1939) *Elementary Number Theory*, New York: McGraw-Hill Book Co.
71. Vallée Poussin, Ch de la (1896) Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20₂: 183-256, 281-297.
72. Vinogradov, A. I. (1965) The density hypothesis for Dirichlet L -series. (Russian). *Izv. Akad. Nauk SSSR, Ser. Math.* 29: 903-934; MR 33, # 5579. [Correction: (1966) *ibid.*, 30: 719-720; MR 33, # 2607.]
73. Vinogradov, I. M. (1937) The representation of an odd number as the sum of three primes. (Russian.) *Dokl. Akad. Nauk SSSR*, 16: 139-142.
74. Vinogradov, I. M. (1954) *Elements of Number Theory*. Translated by S. Kravetz. New York: Dover Publications.
- 74.a Vinogradov, I. (1972) *Fundamentos de la teoría de los números*, (Traducción española de la 7.^a ed. rusa), Ed. MIR, Moscú.
75. Walfisz, A. (1963) *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte, XV, V E B Deutscher Verlag der Wissenschaften, Berlin.
76. Williams, H. C., and Zarnke, C. R. (1972) Some prime numbers of the form $2A3^n + 1$ and $2A3^n - 1$. *Math. Comp.* 26: 995-998; MR 47, # 3299.
77. Wrathall, Claude P. (1964) New factors of Fermat numbers. *Math. Comp.*, 18: 324-325; MR 29, # 1167.
78. Yin, Wen-lin (1956) Note on the representation of large integers as sums of primes. *Bull. Acad. Polon. Sci. Cl. III*, 4: 793-795; MR 19, 16.

Índice de símbolos especiales

- $d|n, d \nmid n$,
 $(a, b), (a_1, \dots, a_n)$,
 $[a, b]$,
 $\mu(n)$,
 $\varphi(n)$,
 $f * g$,
 $I(n) = \left[\frac{1}{n} \right]$,
 f^{-1} ,
 $u(n) = 1$,
 $\Lambda(n)$,
 $\lambda(n)$,
 $\sigma_a(n), \sigma(n), d(n)$,
 $\alpha \circ F$,
 $f_p(x)$,
 $f'(n) = f(n)\log n$,
 C ,
 O ,
 $\sim$,
 $\zeta(s)$,
 $\pi(x)$,
 $\psi(x)$,
 divide (no divide), 16
 máximo común divisor (m.c.d.), 17
 mínimo común múltiplo (m.c.m.), 26
 función de Möbius, 29
 indicatriz de Euler, 30
 convolución de Dirichlet, 35
 función identidad, 36
 inversa de Dirichlet, 37
 función unidad, 38
 función de Mangoldt, 39
 función de Liouville, 46
 funciones divisores, 47
 convolución generalizada, 48
 serie de Bell de f módulo p , 53
 derivada, 56
 Constante de Euler, 66
 rotación O mayúscula, 66
 igualdad asintótica, 66
 función zeta de Riemann, 309
 número de primos $\leq x$, 93
 función ψ de Chebyshev, 94

- $\mathfrak{Y}(x)$,
 $M(x)$,
 o ,
 $a \equiv b \pmod{m}$,
 $\hat{a}$,
 a' ,
 $\chi(n)$,
 $L(1, \chi)$,
 $L'(1, \chi)$,
 $c_k(n)$,
 $G(n, \chi)$,
 $G(k; n)$,
 $nRp, n\bar{R}p$,
 $(n|p)$,
 $(n|P)$,
 $\exp_m(a)$,
 $\text{ind}_g a$,
 $L(s, \chi)$,
 σ_a ,
 σ_c ,
 $\Gamma(s)$,
 $\zeta(s, a)$,
 $F(x, s)$,
 $B_n(x), B_n$,
 $\bar{B}_n(x)$,
 $p(n)$,
 $\omega(n), \omega(-n)$,
 función $\mathfrak{Y}$ de Chebyshev, 94
 sumas parciales de la función de Möbius, 114
 rotación o minúscula, 119
 congruencia, 135
 clase de restos a mód m , 139
 inverso de a mód m , 141
 carácter de Dirichlet, 174
 suma de la serie $\sum \chi(n)/n$, 177
 suma de la serie $-\sum \chi(n) \log n/n$, 186
 suma de Ramanujan, 201
 suma de Gauss asociada a χ , 207
 suma cuadrática de Gauss, 221
 resto cuadrático (no resto) mód p , 223
 símbolo de Legendre, 225
 símbolo de Jacobi, 235
 exponente de a módulo m , 255
 índice de a en base g , 267
 función L de Dirichlet, 279
 abscisa de convergencia absoluta, 280
 abscisa de convergencia, 290
 función gamma, 310
 función zeta de Hurwitz, 309
 función zeta, periódica, 319
 polinomios de Bernoulli (números), 328, 329
 funciones de Bernoulli periódicas, 332
 función de partición, 383
 números pentagonales, 388

Índice alfabético

Abscisa de convergencia absoluta, 280
de convergencia, 290

Abel, identidad de, 96

Abelianos, grupos, 163

Algoritmo de división, 23
de Euclides, 24

Apostol, Tom M., 413

Ayoub, Raymond G., 32, 413

Abel, Niels Henrik, 96

Banda crítica, 365

Bell, Eric Temple, 35, 52, 413

Bell, series de, 53

Bernoulli, números, 329

funciones periódicas, 332

polinomios, 328

Borozdkin, æ. G., 12, 413

Buhstab, A. A., 11, 413

Cálculo de $(-1|p)$, 227

de $(2|p)$, 227

de $\zeta(-n, a)$, 327

de $\zeta(-2n)$, 330

de $L(0, x)$, 332

Cálculos de índices, 267

Carácter principal, 169, 174

Caracteres de Dirichlet, 174

de grupos abelianos, 168

primitivos, 210

Cauchy, Augustin-Louis, 55, 180, 248

Cauchy, producto de, 54

Ceros de la función- L , $L(s, x)$, 341

de función zeta $\zeta(s)$ de Riemann, 340, 365

Ceros triviales de $\zeta(s)$, 322

Clarkson, James A., 22, 413

Clases de restos, 139

Clausen, Thomas, 342

Coefficiente de Fourier, 201

Congruencia binomial, 270

Congruencia cuadrática, 223

Congruencia exponencial, 271

Congruencia lineal, 141, 144, 267

Congruencias, 135

Congruencias polinómicas, 145

Conjetura de Fermat, 13

Conjetura de Goldbach, C., 379

Conjetura de Mertens, 115

Constante de Euler, 66, 311

Convolución de Dirichlet, 35

generalizada, 48

Conductor de un carácter, 214

Criterio de Euler, 225

Chandrasekharan, Komaravolu, 413

Chebyshev, Pafnuti Liwovich, 10, 94

Chen Jing-run, 12, 380, 413

Darling, H. B. C., 406

Davenport, Harold, 413

Definición de grupo, 163

abeliano, 163

cíclico, 166

Demostración elemental del teorema del número primo, 10, 124

Derivada de funciones aritméticas, 56

Desigualdad Pólya para suma de caracteres, 217, 220

Desigualdades, para $|\zeta(s, a)|$, 336

para $|\zeta(s)|$, 336, 357, 363

para $|L(s, x)|$, 338

para $\pi(n)$, 103

para n -ésimo primo p_n , 106

para $d(n)$, 294

- Desigualdades, para $\varphi(n)$, 372
 para $p(n)$, 393, 394
 Dickson, Leonard Eugene, 13, 414
 Dirichlet, carácter $\chi(n)$ de, 174
 convolución (producto), 35
 función- L , 279
 inversas, 37
 orden medio de $d(n)$, 65, 72
 problema del divisor, 75
 series, 279
 teorema sobre primos en las progresiones aritméticas, 8, 183, 193
 Dirichlet, Peter Gustav Lejeune, 6, 8, 35, 66, 174, 183, 279
Disquisitiones Arithmeticae, 6
 Divisibilidad, 16
 División, algoritmo de la, 23
 Divisor, 16
 Ecuación funcional, para (s) , 310
 para $L(s, \chi)$, 326
 para $\zeta(s)$, 322
 para $\zeta(s, h/k)$, 324
 Ecuaciones diofánticas, 5, 239
 Edwards, H. M., 414
 Elemento identidad, 36, 163
 Ellison, W. J., 382
 Erdős, Paul, 10, 414
 Euler, Leonhard,
 Exponente de a módulo m , 255
 Fermat, Pierre de, 6, 8, 13, 143, 144
 Factor, 16
 Fórmula asintótica de Selberg 127, 131
 Fórmula de Hurwitz para $\zeta(s, a)$, 318
 Fórmula de inversión de Möbius, 39
 forma producto de la, 59
 generalizada, 50
 Fórmula del valor medio para series de Dirichlet, 298
 Fracción reducida, 25
 Fórmula de sumación de Euler, 67
 Franklin, Fabian, 391, 414
 Función completamente multiplicativa, 41
 Función gamma, 310
 Función generadora, 384
 Función identidad $I(n)$, 36
 Función indicatriz $\varphi(n)$, 30
 Función- L $L(s, \chi)$, 279
 Función $\lambda(n)$ de Liouville, 46
 Función de Mangoldt $\Lambda(n)$, 39
 Función de Möbius $\mu(n)$, 29
 Función multiplicativa, 41
 Función zeta de Riemann, 309
 Función de teoría de números, 29
 Función zeta de Hurwitz $\zeta(s, a)$, 309
 Función zeta de Hurwitz, 309
 periódica, 319
 Riemann, 309
 Función theta, 382
 Función zeta periódica, 319
 Función aritmética periódica, 197
 Función de partición $p(n)$, 383
 Funciones aritméticas, 29
 Chebyshev $\vartheta(x)$, 94
 Funciones Chebyshev $\psi(x)$, 94
 completamente multiplicativa, 43
 Dirichlet $L(s, \chi)$, 279
 funciones divisores $d(n)$, $\sigma_n(n)$, 47
 indicatriz de Euler $\varphi(n)$, 30
 n -ésima función periódica de Bernoulli $B_n(x)$, 332
 $\kappa(n)$, 307
 $\mu(x)$, 115
 $\nu(n)$, 307
 $\pi(x)$, 9, 93
 $\psi_1(x)$, 345
 Funciones divisor $\sigma_n(n)$, 47
 Funciones μ_k de Möbius de orden k , 63
 Gauss, Carl Friedrich,
 Gerstenhaber, Murray, 233, 414
 Goldbach, C., 7, 10, 379
 Grosswald, Emil, 414
 Grupo conmutativo, 163
 Grupos abelianos, 163
 Hadamard, Jacques, 10, 93, 414
 Hagi, Peter, Jr., 414
 Hardy, Godfrey Harold, 75, 365, 381, 414
 Hemer, Ove, 414
 Hilbert, David, 365
 Hurwitz, Adolf, 309
 Identidad de Abel, 96
 Identidad de Legendre, 84
 Identidad de Selberg, 57
 Identidad del triple producto de Jacobi, 398
 Igualdad asintótica, 66
 Indicatriz de Jordan $J_k(n)$, 60
 Índice, 267
 Índices (tabla de), 268, 269
 Inducción, principio de, 15
 Infinitud de números primos, 19, 22
 Ingham, A. E., 414
 Integración de Riemann-Stieltjes, 97
 Inversos de Dirichlet, 37
 de una función completamente multiplicativa, 44
 Iseki, Kaneshiro, 416
 Jacobi, Carl, Gustav Jacob, 235, 380, 391, 401
 Kloosterman, H. D., 220
 Kolberg, Oddmund, 406
 Kolesnik, G. A., 75
 Knyswijk, D., 406, 409, 414
 Lagrange, Joseph Louis, 6, 146, 194, 199
 Landau, Edmund, 75, 295, 308, 376, 415
 Le Veque, William Judson, 2, 239, 415
 Leech, John, 11, 415
 Legendre, Adrien Marie, 6, 84, 225, 231, 414
 Lehmer, Derrick Henry, 6, 365, 395, 415
 Lehmer, Derrick Norman, 7, 415
 Lema de Euclides, 18
 Lema de Gauss, 228
 Lema Riemann-Lebesgue, 346
 Levinson, Norman, 365, 415

- Ley de reciprocidad cuadrática, 231, 237, 240, 244
 Ley de reciprocidad para los símbolos de Jacobi, 237
 para símbolos de Legendre, 234, 243, 250
 para sumas cuadráticas de Gauss, 251
 Liouville, Joseph, 46
 Littlewood, John Edensor, 11, 381, 415
 Lucas, Edouard, 341
- Máximo común divisor, 17, 24, 25
 McMahon, Percy A., 395
 Medias de funciones aritméticas, 65
 Menor raíz primitiva (tabla de), 266
 Mersenne, P., 5
 Mertens, Franz, 115
 Mills, W. H., 9, 415
 Mínimo común múltiplo, 26
 Möbius, Augustus Ferdinand, 29
 Módulos inducidos, 210
 Mordell, Louis Joel, 381
 Multiplicación de Dirichlet, 36
 de las clases de restos, 173
 Multiplicidad de funciones aritméticas, 35
 de series de Dirichlet, 283
- Nevanlinna, Veikko, 415
 Niven, Ivan, 415
 No-resto cuadrático, 223
 Notación *O*-mayúscula, 66
 Notación *o*-minúscula, 119
 Número perfecto, 4
 Números de Mersenne, 4
 Números pentagonales, 26, 388
 Números poligonales, 2, 6
 Números triangulares, 2, 408
- Orden de un grupo, 164
 Orden medio, 66
 Partición, 379
 Polinomio de interpolación de Lagrange, 199
- Pólya, G., 217
 Prachar, Karl, 415
 Primos, 2, 19
 contenidos en una factorial, 84
 de Fermat, 8
 infinitud, 19, 23
 de Mersenne, 5
 en las progresiones aritméticas, 8, 183, 193
 Primos gemelos, 7
 Primos relativos, 18, 25
 entre sí dos a dos, 25
 Principio de la clasificación cruzada, 155
 Principio de inducción, 15
 Problema de Waring, 382
 Producto de Cauchy, 54
 Productos de Euler, 286
 Prolongación analítica
 de la función zeta de Hurwitz, 316
 de la función zeta de Riemann, 317
 Propiedad de descomposición de los sistemas residuales reducidos, 157
 Puntos reticulares, 72, 78
 visibles, 78
- Rademacher, Hans, 395, 415
 Raíces primitivas, 255
 Ramanujan, Srinivasa, 201, 381, 405, 411
 Recta crítica, 365
 Regiones carentes de ceros de $\zeta(s)$, 363, 364
 Relaciones de ortogonalidad por caracteres, 172
 por caracteres de Dirichlet, 173
 Rényi Alfred, 12, 415
 Resto cuadrático, 223
 Restos y sistemas completos, 139
 reducidos, 143, 157
 Riemann, Georg Friedrich Bernhard, 10, 280, 365, 415
 Robinson, Raphael M., 8, 416
 Rosser, J. Barkley, 366, 416
- Schnirelmann, L., 12, 416
 Selberg, Atle, 10, 51, 127, 416
 Semiplano de convergencia absoluta, 280
 de convergencia 290
 Serie formal de potencias, 52
 Series de Bell, 53
 Shanks, Daniel, 389, 408, 416
 Shapiro, Harold N., 107, 183
 Shen, Mok-Kong, 10, 415
 Sierpinski, Waclaw, 13, 185, 416
 Símbolo, Jacobi ($n|P$), 236
 Legendre ($n|p$), 225
 Símbolo para el mayor entero menor que un número, 9, 29, 68, 91
 Símbolo de Jacobi ($n|P$), 235
 Símbolo ($n|p$) de Legendre, 225
 Sin cuadrados, 25
 Sistema completo de restos, 140
 residual, 143
 Subgrupo, 164
 Subgrupo cíclico, 166
 Suma geométrica, 197, 198
 Sumas de Gauss asociadas a x , 207
 cuadrática, 221, 382
 Suma de Kloosterman, 220
 Suma de Ramanujan, 201, 220
 Sumas separables de Gauss, 207, 214
- Tatuzawa, Tikao, 125
 Teorema de Euler-Fermat, 143
 Teorema de Fermat (pequeño), 144
 Teorema de la factorización única, 20
 Teorema fundamental de Aritmética, 20
 Teorema de la integral logarítmica $Li(x)$, 130
 Teorema de Landau, 295, 308
 Teorema de Lagrange sobre congruencias, 146
 Teorema de los números pentagonales de Euler, 389
 Teorema de los números primos, 10, 81, 93, 99, 106, 123, 124, 345, 359
 Teorema de los números triangulares de Gauss, 408
 Teorema de Wilson, 147
 Teorema de Wolstenholme, 147
 Teorema del resto chino, 148
 Teorema tauberiano de Shapiro, 107
 Teoría aditiva de números, 379
 Teoría multiplicativa de números, 379
 Terna pitagórica, 3

Titchmarsh, Edward Charles, 377, 416

Uspensky, J. V., 416

Valleé-Pousin, C. J. de la, 10, 93, 416

Van der Corput, J. G., 75

Van Lint, Jacobus Hendrieus, 397, 415

Vinogradov, A. I., 12, 416

Vinogradov, I. M., 12, 380, 416

Von Mangoldt, H., 39

Von Standt, Karl Georg Christian, 341

Voronoi, G., 75

Walfisz, Arnold, MM., 115, 416

Waring, Edward, 382

Williams, H. C., 7, 416

Wilson, John, teorema de, 147

Wrathall, Claude P., 8, 416

Wright, E. M., 415

Yin, Wen-lin, 12, 415

Zarnke, C. R., 7, 415

Zuckerman, Herberts, 415

T. M. APOSTOL

**INTRODUCCIÓN A LA
TEORÍA ANALÍTICA DE
LOS NÚMEROS**



EDITORIAL
REVERTÉ

www.reverte.com